

# Blue Ridge HMIS Policies and Procedures



# Table of Contents

Blue Ridge HMIS Policies and Procedures .....	1
Table of Contents .....	2
Overview and Introduction.....	4
POTENTIAL BENEFITS OF BRHMIS .....	5
HANDBOOK FORMAT.....	6
ACKNOWLEDGEMENTS .....	6
HUD HMIS DATA AND TECHNICAL STANDARDS FINAL NOTICE.....	6
DOMESTIC VIOLENCE SHELTERS AND PROGRAMS .....	7
Section 1: Contractual Requirements and Roles .....	8
Policy 1-1: BRHMIS Contract Requirements .....	9
Policy 1-2: BRHMIS Steering Committee .....	9
Policy 1-3: BRHMIS Management .....	11
Policy 1-4: Participating Agency Responsibility .....	12
Policy 1-5: Participating Agency Administrator .....	13
Policy 1-6: User .....	14
Policy 1-7: Training.....	14
Policy 1-8: Amending Policies and Procedures .....	15
Section 2: Participation Requirements .....	17
Policy 2-1: Participation and Implementation Requirements.....	18
Participation Agreement Requirements.....	18
Policy 2-2: Data Security Responsibility .....	19
Policy 2-3: Implementation Requirements.....	20
Policy 2-4: Interagency Data Sharing Agreements .....	20
Policy 2-5: Written Client Consent Procedure for Electronic Data Sharing .....	21
Policy 2-6: Confidentiality and Informed Consent .....	22
Policy 2-7: Universal Data Elements .....	24
Policy 2-8: Information Security Protocols.....	26
Policy 2-9: Connectivity.....	27
Policy 2-10: Maintenance of Onsite (Agency) Computer Equipment .....	27
Policy 2-11: BRHMIS Steering Committee Grievance Procedure .....	28
Client Grievance:.....	28
Grievance by Participating Agencies or a Continuum of Care .....	29
Informal Grievance Procedure .....	29
Formal Grievance Procedure.....	29
Section 3: User, Location, Physical, and Data Access .....	31
Policy 3-1: Access Levels for System Users .....	32
Policy 3-2: Access to Data .....	32
Policy 3-3: Access to Client Paper Records .....	33
Policy 3-4: Unique User ID and Password.....	33
Policy 3-5: Right to Deny User and Participating Agencies' Access .....	34
Policy 3-6: Data Access Control .....	35
Policy 3-7: Using BRHMIS Data for Research.....	36
Section 4: Technical Support and System Availability.....	38
Policy 4-1: Planned Technical Support .....	39
Policy 4-2: Participating Agency Service Request.....	39

Policy 4-3: BRHMIS Staff Availability .....	40
Section 5: Stages of Implementation.....	41
Policy 5-1: Stage 1. Planning .....	42
Policy 5-2: Stage 2. Start-Up and Training .....	42
Policy 5-3: Stage 3. Operational Status.....	43
Section 6: Attachments.....	44
Partnership Agreement .....	45
I. Introduction .....	45
II. Confidentiality .....	45
III. Data Entry and/or Regular Use.....	49
IV. Reports.....	50
V. Proprietary Rights of MetSYS and Database Integrity .....	51
VI. Hold Harmless .....	52
VII. Terms and Conditions.....	52
User Policy, Responsibility, & Code of Ethics .....	54
User Policy .....	54
User Responsibility .....	56
User Code of Ethics.....	58
Worksheet for Planning Cross-Institution Access Rights .....	59
Information Card and Basic Privacy Script.....	60
Facts Sheet.....	62
HMIS Data Collection Statement .....	63
Client Consent for Data Collection .....	64
Client Consent for Release of Information.....	66
List of Acronyms and Abbreviations .....	68
List of Revisions, Additions, and Deletions.....	69

## Overview and Introduction

These Policies and Procedures were developed to guide the operation of the Blue Ridge Homeless Management Information System (BRHMIS). The BRHMIS is an additional tool to help assure that individuals and families who are homeless or at risk of becoming homeless have access to housing and supportive services that are appropriate to their housing, health and human service needs.

The Homeless Management Information System Steering Committee oversees and guides the development and management of the BRHMIS. This BRHMIS Steering Committee is comprised of one representative from the Continuum of Care and participating agencies. Through the direction of these dedicated Steering Committee members, these Policies and Procedures reflect the community's stance on the operation of the BRHMIS. The Council of Community Services is the administrating agency for the Blue Ridge Homeless Management Information System and convenes the Steering Committee.

### **The BRHMIS Steering Committee has as guiding principles that the BRHMIS:**

- Is an implementation which minimizes risk and maximizes benefits for homeless men women and children
- Is designed to respect and meet the needs of consumers
- Is a reliable, flexible and consistent technological system to benefit persons who are homeless or at risk of becoming homeless by providing data that:
  - a. Captures accurate local and regional information about characteristics and service needs, and
  - b. Improves care and access to care by allowing for a fully integrated system of referrals and service delivery to people who are homeless
- Uses a data security approach to information management that balances:
  - a. confidentiality, so that only authorized people see the data;
  - b. integrity, so that data is not modified in any way; and
  - c. availability, so that data is accessible to those who use it when they need it.

An underlying philosophy that has driven the process is respect for the personal data of each individual. Clients must give informed consent to having their data entered into the system. They must also authorize the sharing of their data and specify with whom it may be shared. They may decide not to participate and they may not be denied services for lack of participation.

A goal of the BRHMIS is to inform public policy makers about the extent and nature of homelessness in the Roanoke Valley. This is accomplished through analysis of data that is grounded in the actual experiences of homeless persons and the service providers who assist them in shelters and homeless assistance programs. Information that is gathered via interviews conducted by service providers with consumers is analyzed. The resulting statistics are used to develop an unduplicated count, aggregated (void of any identifying client level information) and made available to policy makers, service providers, advocates, and consumer representatives.

The BRHMIS utilizes web-based software that was selected after much thoughtful investigation.

Through this software homeless service organizations across the area are able to capture information about the clients they serve. BRHMIS staff provides technology, training and technical assistance to users of the system throughout the region.

## ***POTENTIAL BENEFITS OF BRHMIS***

### **For homeless men, women, and children:**

- A decrease in duplicative intake and assessments
- Streamlined referrals
- More coordinated case management
- Improved benefit eligibility determination

### **For case managers:**

- Use of web-based software to assess clients' needs and to inform clients about services offered on site or available through referral.
- Use of on-line resource information to learn about resources that help clients find and keep permanent housing or meet other goals clients have for themselves.
- Improve service coordination when information is shared among case management staff within one agency or with staff in other agencies (with written client consent) who are serving the same clients.

### **For agency and program managers:**

- Improved ability to track client outcomes
- Improved coordination of services, internally among agency programs and externally with other service providers
- Improved data used for preparing reports to funding entities, boards and other stakeholders and advocacy for additional resources
- Aggregate information that can be used in program design and implementation through a more complete understanding of clients' needs and outcomes
- Capacity to automate the generation of numeric statistics for use in HUD APRs

### **For community-wide Continua of Care and policy makers and other advocates:**

- Understanding of the extent and scope of homelessness
- Unduplicated count of clients
- Identification of service gaps
- Utilization of aggregated information for system design
- Development of a forum for addressing community-wide issues
- Enable McKinney-Vento funded organizations to meet the congressional mandate specified in the HUD Data and Technical Standards Final Notice.
- Access to aggregate reports that can assist in completion of the HUD-required gaps chart

- Utilization of the aggregate data to inform policy decisions aimed at addressing and ending homelessness at local, state and federal levels.

## **HANDBOOK FORMAT**

This handbook contains the most current information on the operation of the BRHMIS. It is expected that information will be added, removed and altered as necessary as the program evolves. For this reason the Handbook is in modular form so that outdated information may be easily removed and updated information added. For ease of use pagination is by Section and policy number. Attachments start on page ??.

## **ACKNOWLEDGEMENTS**

This BRHMIS Policy and Procedures Handbook was collaboratively written and reviewed by BRHMIS Steering Committee members Ed McGrath, Dan Merenda, and Gerry Oefelein. We thank the BRHMIS Steering Committee members for their keeping the project on task and for their insightful suggestions.

This Handbook draws heavily (with permission) from the work of the Rhode Island Coalition for the Homeless, the Rhode Island Continuum of Care, the Rhode Island Housing and Mortgage Finance Corporation, and the Connecticut Coalition to End Homelessness HMIS Project. We thank them for their hard work and generosity in letting us adapt their documentation for our use.

December, 2007

## **HUD HMIS DATA AND TECHNICAL STANDARDS FINAL NOTICE**

HUD has issued the Homeless Management Information System (HMIS) Data and Technical Standards Final Notice, dated July 30, 2004. This Notice implements the data and technical standards for the HMIS, and describes baseline requirements for all facets of the HMIS. HUD has provided additional training to interested parties on these required baseline standards.

A subsequent HUD Notice (Docket No. FR 4848-N-03 Homeless Management Information Systems (HMIS) Data and Technical Standards Final Notice; Clarification and Additional Guidance on Special Provisions for Domestic Violence Provider Shelters) clarifies and provides further guidance on the special provisions for domestic violence provider shelters participating in Homeless Management Information Systems (HMIS). It provides clarification and additional guidance on the timing of participation and data collection, submission, and aggregation requirements for HUD McKinney-Vento funded domestic violence shelters.

The privacy and security section in the Notice provides baseline standards required of all programs that record, use or process HMIS data. According to the Notice, these required baseline standards are based on principles of fair information practices and security standards recognized by the information privacy and technology communities as appropriate for securing and protecting personal information and rely on software applications that typically come with hardware purchased within recent years. The Notice further explains that HUD has issued these required baseline requirements and additional security protections that communities may choose to implement to further ensure the security of their HMIS data.

## ***DOMESTIC VIOLENCE SHELTERS AND PROGRAMS***

Domestic Violence Shelters and Programs – those nonprofit organizations whose primary mission is to provide services to victims of domestic violence, dating violence, or stalking – are currently (December 2007) prohibited from entering Protected Personal Information into any HMIS.

If an organization's primary mission is other than those listed above, they may participate in the BRHMIS.

## **Section 1: Contractual Requirements and Roles**

## ***Policy 1-1: BRHMIS Contract Requirements***

---

The Council of Community Services is committed to coordinate and provide services to emergency shelter programs and other HUD funded programs that are required to participate in a HMIS. Participating Agencies shall sign a Partnership Agreement and comply with the stated requirements.

The Council of Community Services will contract for and administer a contract for the following:

- Server based software license (Production and Training Systems)
- User licenses issued
- Training for Software Implementation
- Annual Support agreement
- Disaster Protection and Recovery Support
- 128-bit encryption

Participating Agencies shall sign a Partnership Agreement (page 45 ) and comply with the stated requirements. Agencies will be granted access to the BRHMIS software system after:

- The Partnership Agreement (PA) has been signed with the Council of Community Services, and
- Agencies put into place the stated requirements in the PA.
- Users attend a User Training session, and Site Leaders attend a Program Management workshop.

Agencies agree to comply with the policies and procedures approved by the BRHMIS Steering Committee.

## ***Policy 1-2: BRHMIS Steering Committee***

---

A Steering Committee, convened by the Blue Ridge Regional Continuum of Care, representing stakeholders in the HMIS project, will advise all project activities. The committee meets on a schedule it determines. (A current BRHMIS Steering Committee Membership List may be obtained from the Blue Ridge Regional Continuum of Care).

The BRHMIS Steering Committee guides this project, serves as the decision making body and provides advice and support to the Blue Ridge Regional Continuum of Care.

The BRHMIS Steering Committee will take actions that ensure adequate privacy protection provisions in project implementation.

Membership of the BRHMIS Steering Committee will be established according to the following guidelines:

- The Continuum of Care (CoC) will appoint two individuals who will represent their members and communicate back to them.
- The CoC is responsible to find a replacement for any representative that is participating inconsistently or is inactive.
- The BRHMIS Steering Committee has the authority to add representatives from other sectors of the community in a method it deems appropriate.
- General membership is drawn from volunteers representing the participating agencies.

The BRHMIS Steering Committee has decision making authority in the following areas:

- Determining the guiding principles that should underlie the implementation activities of the BRHMIS, including participating organizations, consumer involvement and service programs;
- Selecting the minimal data elements to be collected by all programs participating in the BRHMIS project;
- Defining criteria, standards, and parameters for the release of aggregate data; and
- Recommending the software vendor to the governing organization.
- Recommending priorities to the Continuum of Care
- Assisting in the identification of funding streams for the HMIS.

As a sub-committee of the Roanoke Continuum of Care, the HMIS Steering Committee follows the protocol of the CoC.

Consensus of the group as a whole is considered by this committee to be the most useful and healthy means of making a decision. However, in the event that a consensus is not forthcoming the following voting regulations will be called upon:

Each association (*human service agency, business, faith organization and public agency*) shall have at least one official representative who attends meetings. Each agency/organization/unit of government that has attended at least one-half of the previous six meetings has one vote. One designee of the official representative may vote in the absence of the official representative.

**Meetings:** The HMIS Steering Committee shall meet monthly and as scheduled by the committee as a whole; Special meetings of the Members may be called by a majority of the Steering Committee.

**Quorum:** Those Members present at a regularly scheduled meeting will constitute a quorum. The act of a majority of the Members present shall be the act of the full Membership.

**Minutes of Meetings:** Minutes shall be kept of every meeting and shall include, at a minimum, the date, time and place of the meeting, the names of all who are in attendance, the topics discussed, the decisions reached and actions taken, any reports made, and any other information as may be deemed necessary by the Chair. The Council of Community Services will keep official copies of the minutes for a minimum of five years or as is standard for HUD documentation.

### ***Policy 1-3: BRHMIS Management***

---

The President of the Council of Community Services is responsible for oversight of all contractual agreements with funding entities, as recommended by the CoC and the BRHMIS Steering Committee.

Governance Procedures:

- The BRHMIS Steering Committee provides recommendations to the Blue Ridge Continuum of Care and the Council of Community Services decisions related to the governance of the BRHMIS. The Council of Community Services is responsible for the day-to-day operation and oversight of the system. Decisions made or actions by the Council of Community Services which do not satisfy an interested party, which may be an agency(ies) or a client(s), may be brought before the BRHMIS Grievance Committee for review. (See Facts Sheet, page 62)
- The Grievance Committee members shall not have a conflict of interest for the grievance they are adjudicating. Membership will consist of the Chair of the Steering Committee, one CoC representative, and three Steering Committee members.

Council of Community Services responsibilities for the operation and oversight of the system include:

- Management of technical infrastructure;
- Planning, scheduling, and meeting project objectives;
- Coordinating training and technical assistance including an annual series of training workshops for end users, agency administrators; and
- Implementing software enhancements recommended by the BRHMIS Steering Committee.

## ***Policy 1-4: Participating Agency Responsibility***

---

Each Participating Agency will be responsible for oversight of all agency staff that generate or have access to client-level data stored in the system software to ensure adherence to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), HUD Department of Housing and Urban Development Docket No. FR-4848-N-02: Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice and all State and Federal regulations as well as to ensure adherence to the BRHMIS principles, policies and procedures outlined in this document.

The Participating Agency:

- Holds final responsibility for the adherence of the agency's personnel to the HIPAA, HUD DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT Docket No. FR-4848-N-02 Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice and all State and Federal regulations as well as ensuring adherence to the BRHMIS principles, policies and procedures outlined in this document;
- Is responsible for all activity associated with agency staff access and use of the BRHMIS data system;
- Is responsible for establishing and monitoring agency procedures that meet the criteria for access to the BRHMIS System, as detailed in the policies and procedures outlined in this document;
- Will put in place policies and procedures to prevent any misuse of the software system by designated staff;
- Agrees to allow access to the BRHMIS System only to staff who have been trained in the BRHMIS system and who have a legitimate need for access. Need exists only for those shelter staff, volunteers, or designated personnel who work directly with (or who supervise staff who work directly with) clients, or have data entry or technical responsibilities; and
- Agrees to follow accepted change control procedures for all configuration changes as outlined in the BRHMIS System Administrators Manual.

The Agency also oversees the implementation of data security policies and standards and will:

- Assume responsibility for integrity and protection of client-level data entered into the BRHMIS system;
- Ensure organizational adherence to the BRHMIS Policies and Procedures;
- Communicate control and protection requirements to agency custodians and users;
- Authorize data access to agency staff and assign responsibility for custody of the data;
- Monitor compliance and periodically review control decisions;
- Ensure that data is collected in a way that respects the dignity of the participants;
- Ensure that all data collected must be relevant to the purpose for which it is used,

- that the data is entered accurately and on time; and
- Provide prompt and timely communications of data, changes in license assignments, and user accounts and software to the BRHMIS Administrator.
- Notify immediately the BRHMIS Administrator of any issue relating to system security or client confidentiality.

### ***Policy 1-5: Participating Agency Administrator***

---

Every Participating Agency shall designate one person to be the Agency Administrator who holds responsibility for the coordination of the system software in the agency.

The Agency Administrator will be responsible for duties including:

- Editing and updating agency information;
- Ensuring that access to the BRHMIS is requested for authorized staff members only after they have:
  - a. received training;
  - b. satisfactorily demonstrated proficiency in use of the software; and
  - c. demonstrated understanding of the Policies and Procedures and agency policies referred to above.
- Granting technical access to the software system for persons authorized by the Agency's leadership by requesting the HMIS Administrator to create passwords and grant licenses needed to enter the system;
- Designating each individual's level of access;
- Ensuring that new staff persons are trained on the uses of the BRHMIS software system, including review of the Policies and Procedures in this document and any agency policies which impact the security and integrity of client information;
- Notifying all users in their agency of interruptions in service;
- Serving as point-person in communicating with the BRHMIS Administrator;
- Facilitating timely reporting from the Agency she/he represents (unless the Agency has designated another person for this function); and
- Working cooperatively with the BRHMIS technical staff and consultants.

The Agency Administrator is also responsible for the implementation of data security policy and standards, including:

- Administering agency-specified business and data protection controls;
- Administering and monitoring access control;
- Providing assistance in and/or coordinating the recovery of data, when necessary;

and

- Detecting and responding to violations of the Policies and Procedures or agency procedures.

The HMIS Administrator will coordinate training and technical assistance for Agency Administrators.

### ***Policy 1-6: User***

.....

All individuals at the participating agency levels who require legitimate access to the software system will be granted such access after training and agency authorization. Individuals with specific authorization can access the system software application for the purpose of conducting data management tasks associated with their area of responsibility.

Responsibilities:

- The BRHMIS Administrator agrees to authorize use of the BRHMIS only to users who have received appropriate training, and who need access to the system for technical administration of the system, data analysis and report generation, back-up administration or other essential activity associated with carrying out BRHMIS responsibilities.
- The Participating Agency agrees to authorize use of the BRHMIS only to users who need access to the system for data entry, editing of client records, viewing of client records, administration or other essential activity associated with carrying out participating agency responsibilities.

Users are any persons who use the BRHMIS software for data processing services. They must be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure. Users are responsible for protecting institutional information to which they have access and for reporting security violations. Users must comply with the data security policy and standards as described and stated by the Agency and HUD baseline requirements stated in the Final Notice Docket No. FR-4848-N-02. Users are accountable for their actions and for any actions undertaken with their usernames and passwords. Users must advise the Agency Administrator and the BRHMIS System Administrator if their passwords are compromised.

Contractors, volunteers, interns and others who function as staff, whether paid or not, are bound by the same User responsibilities and rules set forth in this manual.

### ***Policy 1-7: Training***

---

BRHMIS staff will coordinate ongoing training schedules for Agency Administrators and end Users. Training will occur on a regular basis. The schedule of trainings will be determined by the BRHMIS Steering Committee.

Training schedule:

Basic: Introduction to the BRHMIS System (End User Training)

- Introduction to the BRHMIS Project
- Review of applicable policies and procedures
- Connecting to the Internet
- Logging on to the BRHMIS System
- Entering client information including demographic, placements and services, HUD data and case management

Program Management: Overview of the BRHMIS Project (Agency Administrator)

- Review of agency technical infrastructure including roles and responsibilities
- Review of security policies and procedures
- Overview of agency administrative functions
- Assigning user access levels
- Entering and updating information pertaining to the participating agency
- Review of BRHMIS technical infrastructure
- Reporting with the BRHMIS
  - Introduction to reports
  - Using existing reports
  - Creating new reports
  - Exporting information to other software applications

### ***Policy 1-8: Amending Policies and Procedures***

---

These Policies and Procedures may be amended. It is expected that information will be added, removed and altered as necessary.

The continuum has representation on the BRHMIS Steering Committee. Any changes suggested by any party in the continuum may be presented by a member of the BRHMIS Steering Committee or any Blue Ridge Regional Continuum of Care

BRHMIS staff member to the BRHMIS Steering Committee. A decision on each suggestion will be made according to Policy 1-2.

## **Section 2: Participation Requirements**

## ***Policy 2-1: Participation and Implementation Requirements***

---

### **Participation Agreement Requirements**

Identification of Agency Administrator: Designation of one key staff person to serve as Agency Administrator. The Agency Administrator responsibilities include:

- a. Requesting the creation of usernames and passwords;
- b. Monitoring software access, among other activities;
- c. Ensuring training of new staff persons on how to use the BRHMIS; and
- d. Communicating with the BRHMIS staff about user access and other BRHMIS activities at the agency level.

Security Assessment: Meeting of Agency Executive Director or designee, Program Manager/Administrator (if applicable) and Agency Administrator with BRHMIS staff member to assess and complete Agency Information Security Protocols. Agency IT staff may be asked to participate as necessary.

Training: Commitment of Agency Administrator and designated staff persons to attend training(s) prior to accessing the system online

**NOTE:** ALL Security Information paperwork needs to be complete and signed by Executive Director or designee in order for Participating Agency Staff to attend training.

Interagency Data Sharing Agreements: Interagency Data Sharing Agreements must be established between any shelter/service program where sharing of client level information is to take place. (See the Worksheet for Planning Cross-Institution Access Rights (page 59))

Client Data: Agencies must:

- a. Secure written permission from the client to enter the client's data (page 64) into the BRHMIS.
- b. Secure a release of information from the client to share personal information with other agencies (page 66).
- c. Provide written explanation to each client of how information is to be used and stored (page 60) and on the client's recourse if s/he feels data is misused e.g. grievance policy (page 62). Any incident regarding compromise of client confidentiality must be reported to the BRHMIS staff immediately.

HMIS Signage: The HUD Data and Technical Standard requires as a baseline requirement that every Participating Agency (PA) post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting protected personal information (PPI). While BRHMIS Policy requires written consent, individual Providers may wish to use the following language to assure that they meet this HUD's

baseline standard: “We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required by law or by organizations that give us money to operate this program to collect some personal information. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate”.

Protected Personal Information (PPI) is defined by HUD as “Any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual 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”.

## ***Policy 2-2: Data Security Responsibility***

---

The Council of Community Services will manage the contractual relationship with a third party software development corporation who will in turn continue to develop, implement and maintain all components of operations of the web-based system including a data security program. The BRHMIS Steering Committee, will:

- Define the data security program;
- Implement its standards; and
- Promote awareness of the program to all interested parties.

Access to areas containing HMIS equipment, data, and software will be secured. All client-identifying information will be strictly safeguarded in accordance with appropriate technical safeguards. All data will be securely protected to the maximum extent possible.

The scope of security includes:

- Technical safeguards;
- Physical safeguards, including, but not limited to locked doors;
- Network protocols and encryption standards such as https/ssl encryption (an indicator of encryption use); and
- Client data security (Data Encryption);
- Server and client-side certificates.

## ***Policy 2-3: Implementation Requirements***

---

For Stage 1 implementation, BRHMIS staff will assist Participating Agencies in the completion of all required documentation prior to implementation.

### On Site Security Assessment Meeting:

As defined in Policy 2-1, Agency staff will meet with BRHMIS staff member who will assist in completion of the Agency's Information Security Protocols.

### Partnership Agreement (page 45):

The Partnership Agreement refers to the document agreement made between the participating agency and the BRHMIS project. This agreement includes commitment to enter information on clients served within the agency's participating programs. This document is the legally binding document that refers to all laws relating to privacy protections and information sharing of client specific information.

### User Agreement (page 54):

This form is signed by the case managers and agency administrators to allow them access to the BRHMIS system. Users must participate in training before given live access to the BRHMIS system.

### Identification of Referral Agencies:

The BRHMIS will develop processes to track referrals to agencies not participating in the HMIS.

Participating agency referrals are tracked in the HMIS using the Placement Tool: clients are **placed** into local agency services or **referred** to another agency's services. Reporting tools are available to report these activities.

## ***Policy 2-4: Interagency Data Sharing Agreements***

---

### Responsibilities:

Each agency is responsible for the initiation, negotiation, and completion of Interagency Data Sharing Agreements (page 59) prior to the sharing of information between agencies. Each Executive Director must sign the document to signify his/her agreement and to certify that their internal policies and procedures allow that such an agreement can be made, and that their client consent forms and procedures have been updated to allow for the sharing of client information between the named agencies.

The BRHMIS systems administrator or his/her designee is responsible for providing technical assistance related to system audits as may be required to comply with individual, agency, or government requests.

Written Agreement:

Participating Agencies wishing to share information electronically through the BRHMIS System will provide, in writing, an agreement that has been signed between the Executive Directors of Participating Agencies. Completed agreements will be presented to BRHMIS for review and archival.

- See Interagency Sharing Agreement (page 59).
- Agency staff is responsible for abiding by all the policies stated in the Interagency Sharing Agreement.

Procedure:

- Agencies wishing to participate in a data sharing agreement contact BRHMIS staff to initiate the process.
- Executive Directors complete the Interagency Sharing Agreement. Each participating agency retains a copy of the agreement and a master is filed with the BRHMIS.
- Agency Administrators receive training on the technical configuration to allow data sharing.
- Each Client whose record is being shared must have agreed via a written client consent form to have data shared. A client must be informed both orally and in writing what information is proposed to being shared and with whom it is to be shared.

***Policy 2-5: Written Client Consent Procedure for Electronic Data Sharing***

---

Client Procedures from each Participating Agency, including permission to enter data into the BRHMIS system and release of information for sharing client data, must be on file at each agency.

Each Participating Agency (PA) must publish the BRHMIS privacy notice describing polices and practices for the processing of Protected Personal Information (PPI) and must provide a copy of this privacy notice to any individual upon request. If the PA maintains a web page, the current privacy notice must be posted. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. All amendments to the privacy notice will be consistent with the requirements of these privacy standards. The BRHMIS will maintain permanent documentation of all privacy notice amendments. Lastly, PAs are reminded that they are obligated to provide reasonable accommodations for persons with disabilities

throughout the data collection process. 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. In addition, PAs 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.

The PPI policy will specify the purposes for which it collects PPI and will describe all uses and disclosures. **A PA may use or disclose PPI from the BRHMIS only if the use or disclosure is allowed by the HUD HMIS Final Notice, and is described in this privacy notice. HIPAA regulations receive precedents over the HUD Final Notice PPI policies.** BRHMIS Policy requires written as well as oral consent as a fundamental component of the concept related to informed consent. Except for first party access to information and any required disclosures for oversight of compliance with BRHMIS privacy and security standards, all uses and disclosures are permissive and not mandatory. Uses and disclosures not specified in the privacy notice can be made only with the consent of the individual or when required by law.

A PA must allow an individual to inspect and to have a copy of any PPI about the individual. A PA must offer to explain any information that the individual may not understand. While a PA must consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual, the PA is not required to remove any information but may alternatively choose to mark information as inaccurate or incomplete and may supplement it with additional information. A PA - in accordance with HUD's Final Notice - may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PPI: (1) Information compiled in reasonable anticipation of litigation or comparable proceedings; (2) information about another individual (other than a health care or homeless provider); (3) 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 (4) Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual. Also, a PA may reject repeated or harassing requests for access or correction. A PA 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 protected personal information about the individual.

## ***Policy 2-6: Confidentiality and Informed Consent***

---

Informed consent includes both an oral explanation and written client consent for each client.

### **Oral Explanation:**

All clients will be provided an oral explanation of the BRHMIS. The Participating Agency will provide an oral explanation of the BRHMIS and the terms of consent. The agency is responsible for ensuring that this procedure takes place prior to every client interview. The Oral Explanation must contain the following information: (See page 60)

1. What the BRHMIS is:

- Computer based information system that homeless services agencies across the community use to capture information about the persons they serve

2. Why the agency uses it

- to understand their clients' needs
- help the programs plan to have appropriate resources for the people they serve
- to inform public policy in an attempt to end homelessness

3. Security

- Only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client records

4. Privacy Protection

- No information other than Client profile, HUD required data, and Additional Profile information will be released to another agency without written consent
- Client has the right to not answer any question, **unless entry into a program requires it**
- Client information is transferred in an encrypted format to the BRHMIS database.
- Client has the right to know who has added to, deleted, or edited their BRHMIS electronic client record
- Information that is transferred over the web is through a 128-bit encrypted secure connection

5. Benefits for clients.

- Case manager tells client what services are offered on site or by referral through the assessment process
- Case manager and client can use information to assist clients in obtaining resources that will help them find and keep permanent housing

**Written Client Consent to Enter Data:**

Each client must provide written permission to authorize the agency to enter information into the BRHMIS. (See page 64)

**Written Client Consent to Share Data:**

Each Client whose record is being shared electronically with another Participating Agency must agree via a written client release of data form to have their data shared. A client

must be informed what information is being shared and with whom it is being shared. A client must also be informed of the expiration date of the consent. (See page 66)

**Information Release:**

The Participating Agency agrees not to release client identifiable information to any other organization pursuant to federal and state law without proper client consent.

**Federal/State Confidentiality Regulations:**

The Participating Agency will uphold Federal and State Confidentiality regulations to protect client records and privacy. In addition, the Participating Agency will only release client records with written consent by the client, unless otherwise provided for in the regulations.

1. The Participating Agency will abide specifically by the Federal confidentiality rules regarding disclosure of alcohol and/or drug abuse records.
2. The Participating Agency will abide specifically by the Commonwealth of Virginia’s general laws providing guidance for release of client level information including who has access to client records, for what purpose, and audit trail specifications for maintaining a complete and accurate record of every access to and every use of any personal data by persons or organizations.

**Security:**

The Participating Agency understands that client identifiable data is inaccessible to unauthorized users.

***Policy 2-7: Universal Data Elements***

-----  
 This information is taken from the HUD Standard “Homeless Management Information System (HMIS) Data and Technical Standards Final Notice,” dated July 30, 2004.

Universal data elements are summarized in the following table:

<b>Data standards</b>	<b>Subjects</b>	<b>PPI*</b>	<b>Data entry or computer generated</b>	<b>Collect at initial or every service event</b>
Name	All Clients	Protected	Data Entry	Initial Only
Social Security Number	All Clients	Protected	Data Entry	Initial Only
Date of Birth	All Clients	Protected	Data Entry	Initial Only
Ethnicity and Race	All Clients		Data Entry	Initial Only
Gender	All Clients		Data Entry	Initial Only
Veteran Status	Adults		Data Entry	Every Time
Disabling Condition	Adults		Data Entry	Every Time
Residence prior to Program Entry	Adults & Unaccompanied youth		Data Entry	Every Time
Zip Code of Last Permanent Address	Adults & Unaccompanied youth	Protected	Data Entry	Every Time

Program Entry Date	All Clients	Protected	Data Entry	Every Time
Program Exit Date	All Clients	Protected	Data Entry	Every Time
Unique Personal Identification No.	All Clients	Protected	Computer Generated	Initial Only
Program Identification No.	All Clients	Protected	Computer Generated	Every Time
Household Identifier No.	All Clients		Computer Generated	Every Time

Required response categories for the Universal Data Elements listed above are summarized in the following table:

Name	Response Categories			
	Current Name	First Name	Middle Name	Last Name
Other Name used to Receive Services Previously	First Name	Middle Name	Last Name	Suffix
Example	John	David	Doe	Jr.

Universal Data Element	Response Categories
<b>Social Security Number</b>	
Social Security Number	____.____.____ (example: 123 45 6789)
SSN data quality code	1 = Full SSN reported 2 = Partial SSN reported 8 = Don't Know or Don's have SSN 9 = Refused
<b>Date of Birth</b>	____/____/____ (example: 08/31/1965) Mo/Day/Year
<b>Ethnicity and Race</b>	
Ethnicity	0 = non-Hispanic/Latino 1 = Hispanic/Latino
Race	1 = American Indian or Alaska Native 2 = Asian 3 = Black or African-American 4 = Native Hawaiian or Other Pacific Islander 5 = White
<b>Gender</b>	0 = Female 1 = Male
<b>Veteran Status</b>	0 = No 1 = Yes 8 = Don't Know 9 = Refused
<b>Disabling Condition</b>	0 = No 1 = Yes 8 = Don't Know 9 = Refused
<b>Residence prior to Program Entry</b>	
Type of Residence	1 = Emergency shelter (including a youth shelter, or hotel, motel, or campground paid for with emergency shelter voucher) 2 = Transitional housing for homeless persons (including youth) 3 = Permanent housing for formerly homeless persons (such as SHP, S+C, or SRO Mod Rehab) 4 = Psychiatric hospital or other psychiatric facility 5 = Substance abuse treatment facility or detox center 6 = Hospital (non-psychiatric) 7 = Jail, prison, or juvenile detention facility 10 = Room, apartment, or house that you rent 11 = Apartment or house that you own 12 = Staying or living in a family member's room, apartment, or house 13 = Staying or living in a friend's room, apartment, or house 14 = Hotel or motel paid for without emergency shelter voucher 15 = Foster care home or foster care group home 16 = Place not meant for habitation (e.g. a vehicle, an abandoned building,

	bus/train/subway station/airport or anywhere outside) 17 = Other 8 = Don't Know 9 = Refused
Length of stay in previous place	1 = One week or less 2 = More than one week, but less than one month 3 = One to three months 4 = More than three months, but less than one year 5 = One year or longer
<b>Zip Code of Last Permanent Residence</b>	
Zip code	____ (e.g.12345)
Zip data quality code	1 = Full zip code recorded 8 = Don't know 9 = Refused
<b>Program Entry Date</b>	__/__/____ (example: 08/31/1965) Mo/Day/Year
<b>Program Exit Date</b>	__/__/____ (example: 08/31/1965) Mo/Day/Year
<b>Personal Identification Number</b>	A PIN must be created, but there is no required format as long as there is a single unique PIN for every client served in the CoC and it contains no personally identifying information.
<b>Program Identification Information</b>	
Federal information processing standards (FIPS code)	10-digit FIPS code identifying geographic location of provider (see Part 5 of the Notice for instructions on how to obtain FIPS code)
Facility code	Identification code for facility where services were provided (locally determined)
Continuum of Care code	HUD-assigned
<b>Program Type Code</b>	1 = Emergency shelter (e.g., facility or vouchers) 2 = Transitional housing 3 = Permanent supportive housing 4 = Street outreach 5 = Homeless prevention (e.g., security deposit or one month's rent) 6 = Services only type of program 7 = Other
<b>Household Identification Number</b>	A Household ID number must be created, but there is no required format as long as the number allows identification of clients that receive services as a household.

## ***Policy 2-8: Information Security Protocols***

.....

To protect the confidentiality of the data and to ensure its integrity at the site whether during data entry, storage and review or any other processing function, a Participating Agency must develop at a minimum rules, protocols or procedures to include addressing each of the following:

- Assignment of user accounts
- Unattended workstations
- Physical access to workstations
  - a. The implementation of hardware and/or software firewall to secure local systems/networks from malicious intrusion.
- Use of Antivirus Software, including the automated scanning of files as they are accessed by users on the system where the HMIS application is used as well as

assuring that all client systems regularly update virus definitions from the software vendor.

- Computer Operating Systems are regularly updated for security and critical updates provided by the software vendor.
- Use of Anti-Spy ware, including the automated scanning of files as they are accessed by users on the system where the HMIS application is used as well as assuring that all client systems regularly update virus and spy ware definitions from the software vendor.
- Password complexity, expiration, and confidentiality
- Policy on users including not sharing accounts
- Client record disclosure
- Report generation, disclosure and storage

### ***Policy 2-9: Connectivity***

---

Because vast amounts of data are transmitted, to avoid staff frustration and to be efficient, obtaining and maintaining a broadband (high-speed) Internet connection (greater than 56K/v90) is required. Suggestions include DSL (Digital Subscriber Line), Cable Access, or Satellite Downlink. BRHMIS staff can assist participating agencies to identify Internet providers. However, it is the responsibility of the participating agency to obtain the Broadband Internet connection.

### ***Policy 2-10: Maintenance of Onsite (Agency) Computer Equipment***

---

Executive Director or designee of each participating agency is responsible for the maintenance and disposal of on-site computer equipment and data used for participation in the BRHMIS including the following:

1. Computer Equipment: The Participating Agency is responsible for maintenance of on-site computer equipment. This includes purchase of and upgrades to all existing and new computer equipment for utilization in the BRHMIS Project.
2. Backup: While the BRHMIS system is a server based system, and thus all application level data backups are the vendor's responsibility, each local system is also subject to failure. The Participating Agency is responsible for supporting a backup procedure for each computer connecting to the BRHMIS. A backup procedure may include archival of old existing data, and other general backups of user documents and files.
3. Internet Connection: The Participating Agency is responsible for troubleshooting problems with Internet Connections.

4. Data Disposal: The Participating Agency agrees to dispose of documents that contain identifiable client level data in a manner that will protect client confidentiality. Methods may include:
  - Shredding paper records;
  - Deleting any information from media and destroying the media before disposal; and/or
  - Triple formatting hard drive(s) of any machine containing client-identifying information before transfer of property and/or destruction of hard drive(s) of any machine containing client-identifying information before disposal
5. Data Retention: Protected Personal Information (PPI) that is not in current use seven years after the PPI was created or last changed must be deleted unless a statutory, regulatory, contractual, or other requirement mandates longer retention. Care must be taken to assure that the guidelines associated with Data Disposal are properly followed.

### ***Policy 2-11: BRHMIS Steering Committee Grievance Procedure***

---

The BRHMIS Steering Committee holds the final authority for all decisions related to the governance of the BRHMIS System. Decisions made or actions authorized by BLUE RIDGE REGIONAL CONTINUUM OF CARE regarding the BRHMIS which do not satisfy an interested party, including those at the Continuum, agency or client levels, may be brought before the BRHMIS Grievance Committee for a decision in accordance with the BRHMIS Grievance Procedure.

The Grievance Committee members shall not have a conflict of interest for the grievance they are to adjudicate. Membership will consist of the Chair of the Steering Committee, one CoC representative, and three Steering Committee members.

#### **Client Grievance:**

Clients of participating agencies use the participating agency's existing grievance procedures regarding unsatisfactory services or use and disclosure of Personal Protected Information (PPI) in the BRHMIS, as these issues are most likely within a participating agency. **It is only when the issue involves the actions of the BRHMIS regional operation that the BRHMIS Grievance Procedure is to be used. Additionally, the BRHMIS Grievance Procedure is not intended for use as an "appeal" for a local agency decision.**

If a client wants to file a complaint:

1. The Client complaint is to be brought to the attention of the Participating Agency's Executive Director or designee, who shall assist the client in the Grievance Procedure.
2. The complaint is to be stated in writing.

3. The complaint shall be returned to the BRHMIS party who has the ability and authority to take corrective action. If needed the BRHMIS System Administrator or designee will assist in identifying the appropriate party.
4. The Client and the Participating Agency's representative meet together with the appropriate BRHMIS party to resolve the complaint.
5. The actions and resolutions shall be in writing.
6. If the matter cannot be resolved to the satisfaction of all parties, the BRHMIS Steering Committee will convene the Grievance Committee, giving them information concerning all actions taken to date.
7. The Grievance Committee will meet no later than ten (10) working days after being convened to hear the complaint.
8. The Grievance Committee will resolve the complaint within five (5) working days after meeting.
9. Should the client want to appeal the Grievance Committee's decision, the BRHMIS Steering Committee will hear the complaint at its next scheduled meeting and resolve the complaint in the manner in which it makes its decisions. This decision is final.
10. All actions and resolutions will be in writing. Both the Client and BRHMIS party involved will have a copy describing the resolution of the complaint.

### **Grievance by Participating Agencies or a Continuum of Care:**

Participating Agencies who are participating in the BRHMIS with the Continuum of Care are to first ascertain if the issue is at the Continuum of Care level and if so to resolve it at that level.

If a Participating Agency, Continuum of Care or any combination of such organizations has a complaint about a decision or an action of the BRHMIS staff concerning the BRHMIS or any issue about which the BRHMIS has responsibility, they should first bring the matter to the attention of the BRHMIS System Administrator or designee and/or the party who has the ability and authority to take corrective action as a verbal, informal Grievance Procedure.

### **Informal Grievance Procedure:**

The informal grievance procedure involves bringing the issue verbally to the BRHMIS party who has the ability and authority to take corrective action. It is intended that discussion between the parties shall resolve the issues.

### **Formal Grievance Procedure:**

If the matter is not resolved through the Informal Grievance Procedure to the satisfaction of the Participating Agency or Continuum of Care the Formal Grievance Procedure should be initiated.

1. The complaint should be in writing and submitted to the BRHMIS Steering Committee who will convene the Grievance Committee.
2. The Grievance Committee will meet no later than ten (10) working days after being convened and notified of the complaint and will consider information from all parties involved.
3. The Grievance Committee will hear the complaint from all parties.
4. The Grievance Committee will resolve the complaint within five (5) working days.
5. The actions and resolution of the grievance shall be in writing.
6. If the grieving party is not satisfied, the decision may be appealed to the BRHMIS Steering Committee, who will hear and resolve the complaint at its next regularly scheduled meeting. This decision is final.

## **Section 3: User, Location, Physical, and Data Access**

### ***Policy 3-1: Access Levels for System Users***

---

User accounts will be created and deleted by the BRHMIS Systems Administrator.

Designation of BRIHMIS User Levels: There are different levels of access to the BRHMIS. These levels are reflective of the access a user has to client level paper records. Access levels should be need-based.

A Participating Agency must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (upon hire, and when modified) an end user agreement - as provided in the Attachment section - to acknowledge receipt of a copy of the privacy notice and to pledge to comply with the privacy notice as issued.

### ***Policy 3-2: Access to Data***

---

User access privileges to system data server are stated below.

#### User Access:

Users will be able to view the data entered by Participating Agencies in accordance with their respective Interagency Data Sharing Agreements.. Security measures exist within the BRHMIS software system which restricts agencies from viewing data not covered by an Interagency Data Sharing Agreement. Exceptions are: Client profile, HUD required data, and Additional Profile information.

#### Agency Policies Restricting Access to Data:

The Participating Agencies must establish protocols for internal access to data. These access protocols must contain the following elements:

1. Physical security policies and procedures
2. User security training
  - User orientation
  - Periodic reminders of internal procedures
  - An industry recognized user authentication system
3. Access authorization policies and procedures
4. Access revocation policies and procedures
5. Incident reporting policies and procedures
6. Sanction policies and procedures
7. Termination procedures
8. Risk Assessment

## 9. Risk Management

### ***Policy 3-3: Access to Client Paper Records***

---

Agencies shall follow their existing policies and procedures and applicable local, state and federal regulations for access to client records on paper.

Each agency must secure any paper or other hard copy containing personal protected information that is either generated by or for the BRHMIS, including, but not limited to reports, data entry forms and signed consent forms.

All paper or other hard copy generated by or for the BRHMIS that contains PPI must be directly supervised when the hard copy is in a public area. When agency staff is 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.

All BRHMIS paper records that contain client information must be destroyed seven (7) years after the client has left the program.

### ***Policy 3-4: Unique User ID and Password***

---

**Authorized users will be granted a unique user ID and password:**

- Each user will be required to enter a User ID with a Password in order to logon to the system
- User ID and Passwords are to be assigned to individuals.
- The User ID will be no more than ten characters.
- The Password must be no less than eight and no more than ten characters in length which will not be comprised of words, backward words, names, backward names or any identifiable acronym.
- The password must be alphanumeric.
- Users must use industry standard best practices when selecting their password including the following:
  - a. Use lower and upper case letters
  - b. Do not use passwords containing the names of a spouse, child or pet (similar

names or backward names, places or things) and do not use birthdates or other easy to guess items.

- Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location.

**Password Reset:**

- Initially each user will be given a password for one time use only. The first or reset password will be created by the BRHMIS System Administrator and will be issued to the User by the Systems Administrator, his designee or Agency Administrator. The first time temporary password can be communicated via telephone or in person. Thereafter, passwords will be communicated in verbal form in person or via telephone only to the User. The System Administrator will reset a password if necessary. Passwords will not be sent via e-mail.
- Unsuccessful logon: If a User unsuccessfully attempts to logon three times, the User ID will be “locked out” on the next attempt and access permission will be revoked and user will be unable to gain access until their password is reset in the manner stated above, but only after a verbal request is provided by that user to the BRHMIS Systems Administrator.

All user accounts will be the responsibility of the BRHMIS Systems Administrator.

***Policy 3-5: Right to Deny User and Participating Agencies’ Access***

.....

Participating Agency or user access may be suspended or revoked for suspected or actual violation of the security protocols. Serious or repeated violation by users of the system may result in the suspension or revocation of an agency’s access.

The procedure to be followed is:

1. All suspected violations of any security protocols will be investigated by the agency and the HMIS systems administrator.
2. Any user found to be in violation of security protocols will be sanctioned by his/her agency. Sanctions may include but are not limited to a formal letter of reprimand, suspension of system privileges, revocation of system privileges, termination of employment and/or criminal prosecution.
3. Access may be restricted prior to completion of formal investigation if deemed necessary by the HMIS systems administrator. If access is restricted, the systems administrator will notify the chair of the steering committee of the restriction and will consult with him/her about next steps.
4. Any agency that is found to have consistently and/or flagrantly violated

security protocols may have their access privileges suspended or revoked.

5. All sanctions can be appealed to the Blue Ridge HMIS Steering Committee.

### ***Policy 3-6: Data Access Control***

---

Agency Administrators at Participating Agencies and the HMIS administrator reserve the right to monitor access to system software.

- Agency Administrators at Participating Agencies and the HMIS administrator will regularly review user access privileges and deactivate users when users no longer require access.
- Agency Administrators at Participating Agencies and the HMIS administrator may implement discretionary access controls to limit access to BRHMIS information based on application security designations. Examples of such designations include but are not limited to “Agency Administrator”, “Case Manager”, and “Volunteer”.
- Participating Agencies and the HMIS administrator may audit unauthorized accesses and attempts to access BRHMIS information.
- Audit records shall be kept at least six months, and Agency Administrators and the BRHMIS Systems Administrator may review the audit records for evidence of violations or system misuse.

Guidelines for data access control for the participating agency:

- The federal regulations state that: Physical Access to Systems with access to the BRHMIS Data Computers that are used to collect and store BRHMIS data shall be staffed at all times when in public areas. When workstations are not in use and staff is not present, steps should be taken to ensure that the computers and data are secure and not publicly accessible. These steps should **minimally include:**
  - Logging off the data entry system, shutting down the computer, and storing the computer and data in a locked room

This could be accomplished through the use of an operating system

- such as Windows 2000, or Windows XP Pro, with individual profiles and system security policies enabled
- Each user should have a unique identification code.
- Each user’s identity should be authenticated through an acceptable verification

process.

- Passwords shall be the responsibility of the user and shall not be shared with anyone.
- Users are able to select and change their own passwords, and should do so at least every ninety days.
- Any passwords written down should be securely stored and inaccessible to other persons. Users should not store passwords on a personal computer for easier log on.

### ***Policy 3-7: Using BRHMIS Data for Research***

---

Agencies participating in the BRHMIS should collect personal client information only when appropriate to provide services and/or for other specific purpose of the organization and/or when required by law. Purposes for which agencies collect protected personal information may include the following:

- a. to provide or coordinate services to clients
- b. to locate other programs that may be able to assist clients
- c. for functions related to payment or reimbursement from others for services that are provided
- d. to operate the agency, including administrative functions such as legal, audits, personnel, oversight, and management functions
- e. to comply with government reporting obligations
- f. when required by law
- g. for research purposes

#### **BRHMIS Release of Data for Research Conditions:**

- No client protected personal information for any reason may be released to unauthorized entities.
- Only de-identified aggregate data will be released.
- Aggregate data will be available in the form of an aggregate report or as a raw data set. Parameters of the aggregate data, that is, where the data comes from and what it includes will be presented with each report.
- Research results will be reported to the BRHMIS Steering Committee prior to publication, for publication approval by the BRHMIS Steering Committee.

- Research will be shared with the appropriate agencies after publication.
- BRHMIS Steering Committee will be granted the rights to utilize all findings (results).

The BRHMIS Steering Committee will review and respond to requests for the use of BRHMIS data for research.

## **Section 4: Technical Support and System Availability**

### ***Policy 4-1: Planned Technical Support***

---

The HMIS Administrator, in conjunction with Agency Administrators and contracted third parties, will coordinate technical support services on a planned schedule with each participating agency to:

- Assist Participating Agencies on the use of Entry/Exit forms and other paperwork
- Conduct on-site follow-up training if needed
- Coordinate follow-up data entry training if needed
- Review report generation
- Coordinate ongoing technical assistance as needed
- Assist agencies with network and end user computer security
- Create custom reports, in accordance with BRHMIS Steering Committee guidelines.

### ***Policy 4-2: Participating Agency Service Request***

---

To effectively respond to service requests, the following methods of communicating a service request from a Participating Agency to the HMIS Administrator have been developed:

- Service Request from Participating Agency
  1. End user informs Agency Management Staff (Executive Director/designee or Agency Administrator) of the problem.
  2. Agency Management Staff attempts to resolve issue. If unable to resolve, agency staff may contact HMIS Administrator directly in order to request expedited service.
  3. HMIS Administrator determines resources needed for service and if necessary, contacts vendor for support.
  4. HMIS Administrator contacts agency management staff to work out a mutually convenient service schedule and resolution to issue or concern.
- Chain of communication: (Problems should be resolved at the lowest possible level to assure minimum time to resolution). (Issues resolved at the higher level

will be communicated back through the chain in reverse order.)

1. End User
2. Agency Staff
3. HMIS Administrator
4. Vendor

### ***Policy 4-3: BRHMIS Staff Availability***

---

Consistent with the user's reasonable service request requirements, HMIS Administrator is available for Technical Assistance, questions, and trouble-shooting between the hours of 8:15 AM and 4:30 PM Monday through Friday.

**Emergency Situations:** Outside of normal business hours (8:15 AM to 4:30 PM Monday through Friday), contact the 2-1-1 Information and Referral Center for assistance. They will communicate your emergency to the appropriate BRHMIS staff.

## **Section 5: Stages of Implementation**

### ***Policy 5-1: Stage 1. Planning***

---

Prior to beginning Stage 1, a Participating Agency needs to have:

1. Completed security assessment, including all participation and data sharing agreements as well as client consent protocols;
2. Identified an Agency Administrator; and
3. Made proper connectivity arrangements. Because there is a great quantity of data transfer, the BRHMIS requires that the participating agency have a Broadband Internet connection greater than 56K/90v. This includes DSL, Cable or Satellite Internet access. This Broadband Internet connection requirement will avoid lost staff time and staff frustration.

During Stage 1 of implementation of the BRHMIS:

1. Participating Agency staff and BRHMIS staff meet for the Security Assessment meeting.
2. BRHMIS staff and Agency Administrator will arrange a follow-up site visit to conduct operative tests on the program's equipment, should this be needed.

Indicators to exit Stage 1: The Participating Agency must complete all Stage 1 Activities before moving onto Stage 2 including signed PA (Partnership Agreement) and Data Sharing Agreements returned to the BRHMIS System Administrator.

### ***Policy 5-2: Stage 2. Start-Up and Training***

---

To enter Stage 2, the Participating Agency needs to have completed Stage 1.

Activities during Stage 2 of implementation:

- BRHMIS Administrator creates user IDs and temporary passwords for all users.
- Site users and the Agency Administrator receive training on uses of the BRHMIS application. The Administrator training will include Program and Services Management.
- Trained agency staff work to enter client data into the system using the processes taught during training. These are different for HUD-funded agencies and non-HUD-funded agencies.

The BRHMIS Stage 2 continues until data has been entered on 100% of clients served or for an entire month for all clients served within the Participating Agency. This includes

both basic client data, and program / service data required to support production of the HUD APR or other required reports.

Indicators to exit Stage 2:

- Interview protocols have been established including:
  - a. Implementation of standard default interview protocols,
  - b. Use of interview protocols and
  - c. Data entry including Entry and Exit transactions.
- Data have been entered on 100% of all new or current clients served within participating programs or for an entire month for all clients served within the Participating Agency.
- Agency services have been defined in the HMIS and clients are being placed into them for an entire month.

Participating Agencies need to complete all Stage 2 Activities before moving onto the final Stage 3.

### ***Policy 5-3: Stage 3. Operational Status***

---

To enter Stage 3 data entry must be completed for 100 % of clients served **or** for an entire month on all clients served.

Stage 3 of implementation:

- Begins when staff utilizes the BRHMIS System application to maintain client records, including service information.

Benefits of Stage 3 include the fact that client and service data becomes available for reporting purposes. Reports can be more easily generated such as:

- Standard reports including the HUD APR
- Demographics, including income sources, amounts and non-cash benefits
- Residential history patterns

Participating Agencies will receive support from BRHMIS staff to complete all stages. To ensure that all parties are comfortable with the process and progress for this stage, the Participating Agency and BRHMIS staff may meet again to assess if obstacles to progress exist.

## **Section 6: Attachments**

**Continuum of Care /Homeless Management Information System (HMIS)  
Partnership Agreement  
Between Council of Community Services And [Name]**

This agreement is entered into on \_\_\_\_\_ (d/m/y) between the Council of Community Services, hereafter known as the “CCS” and \_\_\_\_\_ (agency name), hereafter known as “Agency”, regarding access and use of the HMIS Database.

The Executive Director of the Agency must indicate agreement with the terms set forth below by signing this Agreement before a HMIS account can be established for the Agency.

**I. Introduction**

The HMIS Database is a shared homeless database that allows authorized personnel at HMIS Database Member Agencies throughout the Blue Ridge region to share information on common clients. Goals of the Database include: ability to expedite client intake procedures, improved referral activity, increased case management and administrative tools, and the creation of a tool to follow demographic trends and service utilization patterns of families and individuals experiencing homelessness or those families and individuals on the verge of homelessness.

The project is administered by the Council of Community Services with MetSYS, Inc. [Sacramento, CA] housing the central server that hosts the Database and limits access to the database to member Agencies participating in the project. The Council of Community Services intends to protect the HMIS Database data to the utmost of its ability from accidental or intentional unauthorized modification, disclosure, or destruction, and CCS will accomplish this by utilizing a variety of methods to guard the data.

Ultimately, when used correctly and faithfully by all involved parties, the HMIS Database is designed to benefit multiple stakeholders, including the community, homeless service agencies, and the consumer of homeless services, through a more effective and efficient service delivery system.

**II. Confidentiality**

The Agency will uphold relevant Federal, State and local confidentiality regulations and laws that protect client records, and the Agency will only release confidential client records with written consent by the client, or the client’s guardian, unless otherwise

provided for in the regulation or laws. A client is anyone who receives services from the Agency and a guardian is one legally in charge of the affairs of a minor or of a person deemed incompetent.

The Agency shall abide by all local, state and federal confidentiality laws and regulations pertaining to: 1) all medical conditions, including mental illness, alcohol and/or drug abuse, HIV/AIDS diagnosis and other such covered conditions; and 2) a person's status as a victim of domestic violence. A general authorization for the release of medical or other information is NOT sufficient for this purpose.

The agency will abide specifically by federal confidentiality regulations as contained in the Code of Federal Regulations, 42 CFR Part 2, regarding disclosure of alcohol and/or drug abuse records. In general terms, the federal regulation prohibits the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Agency understands that federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.

The Agency will abide specifically with the Health Insurance Portability and Accountability Act of 1996 and corresponding regulations passed by the U.S. Department of Health and Human Services. In general, the regulations provide consumers with new rights to control the release of medical information, including advance consent for most disclosures of health information, the right to see a copy of health records, the right to request a correction to health records, the right to obtain documentation of disclosures of their health information, and the right to an explanation of their privacy rights and how information may be used or disclosed. The current regulation provides protection for paper, oral, and electronic information.

The Agency shall provide a verbal explanation of the HMIS database and the terms of consent to the Clients and shall arrange for a qualified interpreter or translator in the event that an individual is not literate in English or has difficulty understanding the Consent form.

The Agency will not solicit or input information from clients into the HMIS Database unless it is essential to provide services or conduct evaluation or research.

The Agency will not divulge any confidential information received from the HMIS Database to any organization or individual without proper written consent by the client unless otherwise permitted by relevant regulations or laws.

The Agency will ensure that all persons who are issued a User Identification and Password to the HMIS Database within that particular agency abide by this Partnership Agreement, including the confidentiality rules and regulations. The Agency will ensure that each person granted HMIS Database access at the Agency receives a HMIS Database

operational manual. This manual will include information on how to use the HMIS Database as well as basic steps to ensure confidentiality. The Agency will be responsible for managing any of its own requirements that individual employees comply with HMIS Database confidentiality practices, such as having employees sign a consent form stating their understanding of and agreement to comply with HMIS Database confidentiality practices.

Any staff, volunteer or other person who has been granted a User ID and password and is found to have willfully committed a breach of system security and/or client confidentiality shall have his or her access to the database revoked immediately. Any person who has been granted a User ID and password that is found to have committed a negligent breach of system security and/or client confidentiality after a prior warning and correction shall have his or her access to the database revoked immediately. A revoked user may be subject to discipline by the Agency pursuant to the Agency's personnel policies.

In the event of a breach of system security or client confidentiality, the Agency Director shall notify Project Manager at 985-0131 within 24 hours of knowledge of such breach. Any Agency that is found to have had breaches of system security and/or client confidentiality shall enter a period of probation, during which technical assistance shall be provided to help the Agency prevent further breaches. Probation shall remain in effect until the Program Director has evaluated the Agency's security and confidentiality measures and found them compliant with the policies stated in this Agreement and the User Policy, Responsibility Statement, and Code of Ethics Agreement. Subsequent violations of system security may result in suspension from the system.

The Agency understands that the file server, which will contain all client information, including encrypted identifying client information, will be physically located in a locked office with controlled access at the offices MetSYS, Inc., 3835 North Freeway Blvd., Suite 250, Sacramento, CA 95834.

The Agency agrees to maintain appropriate documentation of client consent or guardian-provided consent to participate in the HMIS Database.

The Agency understands that informed client consent is required before any basic identifying client information is entered into the HMIS Database for the purposes of interagency sharing of information. Informed client consent will be documented by completion of the standard HMIS Database Authorization to Release and Exchange Basic Information for the Database form.

The Client Authorization form mentioned above, once completed, authorizes basic identifying client data to be entered into the HMIS Database, as well as non-confidential service transaction information. This authorization form permits basic client identifying information to be shared among all HMIS Database Member Agencies and non-confidential service transactions with select HMIS Database member agencies, based on relevance.

If a client denies authorization to share basic identifying information and non confidential service data via the HMIS Database, identifying information shall only be entered into the HMIS Database if the client information is locked and made accessible only to the entering agency program, therefore, precluding the ability to share information.

The Agency will incorporate a HMIS Database Clause into existing Agency Authorization for Release of Information form(s) if the Agency intends to input and share confidential client data with the HMIS Database. The Agency's modified Authorization for Release of information form(s) will be used when offering a client the opportunity to input and share information with the HMIS Database beyond basic identifying data and non-confidential service information. The Council of Community Services will conduct periodic audits to enforce informed consent standards.

The Agency agrees to place all Client Authorization for Release of Information forms related to HMIS Database in a locked file cabinet to be located at the Agency's business address and that such forms be made available to CCS for period audits. The Agency will retain these HMIS Database related Authorization for Release of Information forms for a period of 5 years, after which time the forms will be discarded in a manner that ensures client confidentiality is not compromised.

The Agency understands that in order to update, edit, or print a client's record, the Agency must have on file a current authorization from the client as evidenced by a completed standard HMIS Database Authorization to Release form pertaining to basic identifying data, and/or a modified Agency form with a HMIS Database Clause pertaining to confidential information.

The Agency understands CCS does not require or imply that services be contingent upon a client's participation in the HMIS Database.

The Agency and CCS understand the HMIS Database Project, and CCS as administrator, are custodians of data and not owners of data.

In the event the HMIS Database project ceases to exist, member Agencies will be notified and provided reasonable time to access and save client data on those served by the agency as well as statistical and frequency data from the entire system. Then, the information collected by the centralized server, located at the MetSYS, Inc., Sacramento, CA, will be purged, or stored. If the latter occurs, the data will remain in an encrypted and aggregate state.

In the event CCS ceases to exist, the custodianship of the data will be transferred to another non-profit for administration, and all HMIS Database Member Agencies will be informed in a timely manner.

### **III. Data Entry and/or Regular Use**

User identification and passwords are not permitted to be shared among users.

If an Agency has access to a client's basic identifying information, non-confidential service transactions, and confidential information and service records, it will be generally understood that a client gave consent for such access. However, before an agency can update, edit, or print such information, it must have informed client consent, evidenced by a current standard HMIS Database Authorization to Release form in writing pertaining to basic identifying data and/or an Agency-modified form with a HMIS Database Clause pertaining to confidential information.

If a client has previously given permission to multiple agencies to have access to her/his information, beyond basic identifying information and non-confidential service transactions, and then chooses to eliminate one or more of these agencies, the Agency at which such desire is expressed will contact its partner agency/agencies with whom the client previously granted permission to exchange and explain that the record, or portions of the record, will no longer be shared at the client's request. The agency where the request is made will then either close the entire record, or simply lock out portions of the record to the other agency or agencies.

In the event that a client would like to rescind consent to participate in the HMIS Database completely, the agency at which her/his desired is expressed, will work with the client to complete a brief form which will be sent to the System Administrator to inactivate the client.

The Agency will only enter individuals in the HMIS Database that exist as clients under the Agency's jurisdiction.

The Agency will not misrepresent its client base in the HMIS Database by entering known inaccurate information (i.e., Agency will not purposefully enter inaccurate information on a new record or to override information entered by another agency).

The Agency will consistently enter information into the HMIS Database and will strive for real-time, or close to real-time, data entry.

The Agency understands that with a current standard HMIS Database Authorization for Release form on file, it can update, edit, and print a client's basic identifying information.

The Agency understands that a modified agency Authorization to Release Information form, with the added HMIS Database clause, permits it to share confidential client information with select agencies.

The Agency understands that assessment screens are only allowed to be edited by the individual that originally enters the data, whether that individual is employed by the Agency or another Member Agency. The Agency will create a separate assessment, as

needed, to indicate a change in a client's status, updates, and to edit incorrect information.

Discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex, and sexual orientation are not permitted in the HMIS Database.

Offensive language and profanity are not permitted in the HMIS Database.

The Agency will utilize the HMIS Database for business purposes only.

The Agency understands the Council will provide initial training and periodic updates to that training to assigned Agency staff about the use of the HMIS Database and confidentiality; this information is then to be communicated to other HMIS Database-using staff within the Agency.

The Agency understands the Council will be available for Technical Assistance (TA) within reason (i.e. troubleshooting and report generation). Standard operating hours in which TA will generally be available are 9:00 AM to 5:00 PM Monday through Friday.

The Agency will keep updated virus protection software on Agency computers that access the HMIS Database.

Transmission of material in violation of any United States Federal or State regulations is prohibited and includes, but is not limited to: copyrighted material, material legally judged to be threatening or obscene, and material considered protected by trade secret.

The Agency will not use the HMIS Database with intent to defraud the Federal, State, or local government, or any individual entity, or to conduct any illegal activity.

The Agency recognizes the Blue Ridge Continuum of Care Committee (Committee), serving the cities of Roanoke and Salem and Roanoke County, to be the discussion center regarding the HMIS Database, including Database process updates, policy and practice guidelines, data analysis, and software/hardware upgrades. The Agency will designate an appropriate person from their staff to attend meetings related to HMIS Database issues on a regular basis.

#### **IV. Reports**

The Agency understands that it will retain access to all identifying and statistical data on the clients it serves.

The Agency understands that access to data on those it does not serve will be limited to basic identifying and non-confidential service data. Therefore, the Agency understands that, with rare exception, a list of all persons in the HMIS Database along with basic identifying information and non-confidential service data can be generated.

Reports obtaining information beyond basic identifying data and non-confidential services on individuals not served by the Agency are limited to statistical and frequency reports, which do not disclose identifying information.

## **V. Proprietary Rights of MetSYS and Database Integrity**

The Agency will not give or share assigned user identification and passwords to access the HMIS Database with any other organization, governmental entity, business or individual.

The Agency will not cause corruption of the HMIS Database in any manner or way. Any unauthorized access or unauthorized modification to computer system information or interference with normal system operations, whether on the equipment housed by CCS or any computer system or network accessed by MetSYS will result in immediate suspension of services, and CCS and/or MetSYS will pursue all appropriate legal action.

## **VI. Hold Harmless**

The Council of Community Services makes no warranties, expressed or implied. The Agency at all times, will indemnify and hold CCS harmless from any damages, liabilities, claims, and expenses that may be claimed against the Agency; or for injuries or damages to the Agency or another party arising from participation in the HMIS Database; or arising from any acts, omission, neglect, or fault of the Agency or its agents, employees, licensees or clients, or arising from the Agencies failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This Agency will also hold CCS harmless for negative repercussions resulting in the loss of data due to delays, non-deliveries, misdeliveries, or service interruption caused by the Agency's or another Member Agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/or acts of God. CCS shall not be liable to the Agency for damages, losses, or injuries to the Agency or another party other than if such is the result of gross negligence or willful misconduct of CCS.

The Agency agrees to keep in force a comprehensive general liability insurance policy with combined single limit coverage of not less than five hundred thousand dollars (\$500,000). Said insurance policy shall include coverage for theft or damage of the Agency's hardware and software, as well as coverage for the Agency's indemnification obligations under this agreement.

## **VII. Terms and Conditions**

The parties hereto agree that this agreement is the complete and exclusive statement of the agreement between parties and supersedes all prior proposals and understandings, oral and written, relating to the subject matter of this agreement.

No party shall transfer or assign any rights or obligations without the written consent of the other parties.

This agreement shall remain in force until revoked in writing by either party, with 30 days advance written notice. The exception to this term is if allegations or actual incidences arise regarding possible or actual breeches of this agreement. Should such situations arise, CCS may immediately suspend access to the HMIS Database until the allegations are resolved in order to protect the integrity of the system.

This agreement may be modified or amended by written agreement executed by both parties with 30 days advance written notice.

Use of the HMIS Database constitutes acceptance of these Terms and Conditions.

---

Executive Director's Signature

Date

---

Executive Director Printed Name

---

Name of Agency

---

Address of Agency

---

Pamela Kestner-Chappelear  
President  
Council of Community Services  
502 Campbell Avenue, SW  
Roanoke, Virginia 24016

Date

## ***User Policy, Responsibility, & Code of Ethics For Blue Ridge Homeless Management Information System (BRHMIS)***

### **User Policy**

In 2001, the United States Congress directed the United States Department of Housing and Urban Development to “collect an array of data on homelessness in order to prevent duplicate counting of homeless persons, and to analyze their patterns of use of assistance, including how they enter and exit the homeless assistance system and the effectiveness of the systems<sup>1</sup>.”

The Blue Ridge Homeless Management Information System (BRHMIS) is a collaborative effort among helping agencies to document client-level needs and characteristics through a coordinated system which aggregates common information at the agency, community, and state levels.

The BRHMIS is a tool that can also assist agencies in focusing services and locating alternative resources to help homeless persons. Agency staff may use the Client information in the system to target services to the Client’s needs.

BRHMIS is an entirely web-based system -- hosted on a remote server -- coordinated by the Council of Community Services. The system is accessed via the Internet by provider sites offering shelter, housing, and supportive services to homeless individuals and families.

Participating Agencies may choose to share information for provision of services to homeless persons through a networked infrastructure that establishes electronic communication among the Participating Agencies.

Participating Agencies shall at all times have rights to the data pertaining to their clients that they directly enter into the BRHMIS system. Participating Agencies shall be bound by all permissions and restrictions imposed by Clients pertaining to the use of personal data for which they have signed a BRHMIS Client Release of Information form.

All BRHMIS Users are required to attend HMIS training sessions prior to using the system.

All BRHMIS Users are required to complete a privacy training specific to protecting information contained within BRHMIS prior to using the System.

All BRHMIS Users are required to have read and understand their Agency’s Privacy Notice.

## Data-Sharing and Release of Information

1. The Agency understands that informed client consent is required before any basic identifying client information is entered into the BRHMIS for the purposes of interagency sharing of information. Informed client consent will be documented by completion of a Client Release of Information.
2. The Client Release form authorizes basic identifying client data entered into the BRHMIS Profile screen to be shared among all BRHMIS Member Agencies and other Assessment and Service Information to be shared with select BRHMIS Member Agencies, based on inter-agency sharing agreements.
3. If a client denies authorization to share personal or other assessment information via the BRHMIS, the staff entering the information shall mark the data as “Local Only”. This assures that client information is accessible only to the agency entering data into the program, therefore, precluding the ability to share information with other agencies. If the client’s name represents an identification risk even if the record is completely closed and the name can only be seen by the entering Agency, the staff may use the “anonymous” client function.

**Minimum data entry on each Client will be defined by your Agency’s Workflow. However, all agencies are encouraged to complete the follow sections of the database:**

- The Common Intake task.
- The Client Release task.
- The HMIS Intake (Universal Data) task.
- The HUD Homeless Characteristics task.
- Client Placements (recorded either in the Placements task or the Case Record form) - information on the client’s needs and how those needs were met.

## Restricted Information

Information, including progress notes and psychotherapy notes, about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV, or AIDS, and domestic violence concerns shall not be shared with other Participating Agencies without the client’s written, informed consent as documented on the Client Consent for Release of Information.

When recording referrals made for these types of services and to agencies that specifically provide these services, the Client’s Service Record shall not be shared with other agencies on the Blue Ridge HMIS system without the Client’s informed consent as documented on the Client Consent for Release of Information. This information should also not be entered in any “open” notes sections in the Blue Ridge HMIS system.

The sharing of information on children under the age of 18, who are not accompanied by a legal guardian, will be governed by existing Agency policy regarding the age at which children under the age of 18 may authorize release of information.

## User Responsibility

Your User ID and Password give you access and authority to use the BRHMIS. Initial each item below to indicate your understanding and acceptance of the proper use of your User ID and password. Failure to uphold the confidentiality standards set forth below is grounds for immediate termination of User privileges.

**Please initial each item below to indicate your acceptance and understanding of the user responsibilities below**

\_\_\_\_\_ I have read and understand my Agency's Privacy Notice.

\_\_\_\_\_ My User ID and Passwords must be kept secure and are not to be shared with anyone, including other staff members.

\_\_\_\_\_ I understand that the only individuals who can view information in the BRHMIS are authorized users and the Client to whom the information pertains. BRHMIS users must respect the privacy and hold in confidence all information obtained in the course of their use of the software system.

\_\_\_\_\_ I may only view, obtain, disclose, or use the database information that is necessary to perform my job.

\_\_\_\_\_ Client information should be accessed only in order to retrieve data relevant to a client requesting services from my agency.

\_\_\_\_\_ I understand that in the event that I am terminated or leave my employment with this agency, my access to the BRHMIS will be revoked.

\_\_\_\_\_ Clients have the right to see their information on BRHMIS. If a client requests to see their information, the Participating Agency/User who receives the request must review the information with the client.

\_\_\_\_\_ I understand that failure to log off BRHMIS appropriately may result in a breach in client confidentiality and system security.

\_\_\_\_\_ If I am logged into BRHMIS and must leave the work area where the computer is located, I must log-off of the BRHMIS before leaving the work area.

\_\_\_\_\_ I understand that my access to BRHMIS is limited to my designated work site unless I am given expressed written consent of the Agency Administrator to access the system from other specified locations.

\_\_\_\_\_ A computer that has BRHMIS "open and running" shall never be left unattended.

\_\_\_\_\_ A computer that has BRHMIS “open and running” shall never be arranged so that unauthorized individuals may see the information on the screen.

\_\_\_\_\_ Hard copies and downloads of information from the BRHMIS onto a hard drive or disk must be kept secure to ensure that only appropriate agency staff has access.

\_\_\_\_\_ When hard copies and “downloads” of BRHMIS Client information are no longer needed, they must be properly destroyed as described in your agency’s privacy and confidentiality policies.

\_\_\_\_\_ If I notice or suspect a security breach, I must immediately notify my Agency Administrator for the BRHMIS and my Executive Director or the BRHMIS System Administrator.

\_\_\_\_\_ I understand that I am responsible for reporting any system malfunctions or “bugs” that I notice or suspect to the Agency Administrator and other appropriate system support staff.

\_\_\_\_\_ I understand that I must secure BRHMIS information as “local only” in each of the modules for which the Client has not given consent for data sharing.

\_\_\_\_\_ I must get a second specific “Release of Information” to share restricted information about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV, AIDS, and domestic violence. In addition, BRHMIS settings must reflect the Client’s expressed wishes as documented through the Informed Consent process.

---

BRHMIS User Signature

Date

---

BRHMIS Agency/System Administrator Signature

Date

---

Agency Director

Date

## User Code of Ethics

Blue Ridge HMIS Users must treat Participating Agencies with respect, fairness and good faith.

Each Blue Ridge HMIS User shall maintain high standards of professional conduct in his/her capacity as a Blue Ridge HMIS User.

All Blue Ridge HMIS Users shall endorse and maintain the client's rights related to privacy and confidentiality and shall adhere to BRHMIS Policies and Procedures.

The Blue Ridge HMIS User has primary responsibility for his/her Client(s).

The Blue Ridge HMIS Users will not misrepresent its client base in the Blue Ridge HMIS system by entering knowingly inaccurate information (i.e. User will not purposefully enter inaccurate information on a new record or to over-ride information entered by another agency.)

Discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex, and sexual orientation are not permitted in the Blue Ridge HMIS system

The User will not use the Blue Ridge HMIS system with intent to defraud the federal, state, or local government or an individual entity; or to conduct any illegal activity.

I understand and agree to comply with all the statements listed above.

---

Blue Ridge HMIS User Signature

Date

---

Blue Ridge HMIS Agency/System Administrator Signature

Date

---

Agency Executive Director

Date

## Worksheet for Planning Cross-Institution Access Rights

Institution Setting Access: \_\_\_\_\_  
 Partner Organization[s] Receiving Access Defined on This Worksheet:  
 All Partners       Partners Listed Below:  
 \_\_\_\_\_  
 \_\_\_\_\_  
 \_\_\_\_\_

See Other Side for Additional Organizations

Global Access:                       No Access  Some Access [See Below]

### Primary Settings:

<b>Global Settings</b> [Other than Fields]:			
View:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	Edit: <input type="checkbox"/> Yes <input type="checkbox"/> No
Add:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	Delete: <input type="checkbox"/> Yes <input type="checkbox"/> No

<b>Global Field Settings:</b>			
View:	<input type="checkbox"/> Yes	<input type="checkbox"/> No	Edit: <input type="checkbox"/> Yes <input type="checkbox"/> No

### Secondary Override Settings:

#### Client Data:

<b>Overall Settings:</b>
<input type="checkbox"/> Share <b>NO</b> Client Data [Block All]
<input type="checkbox"/> Share <b>ALL</b> Client Data [Share Everything]

<b>Override Settings for Client Data:</b>
<input type="checkbox"/> Yes <input type="checkbox"/> No Client Names and IDs
<input type="checkbox"/> Yes <input type="checkbox"/> No Client Addresses and Phones
<input type="checkbox"/> Yes <input type="checkbox"/> No General Client Demographics
<input type="checkbox"/> Yes <input type="checkbox"/> No Financial, Educational and Employment Data
<input type="checkbox"/> Yes <input type="checkbox"/> No Medical and Health Data
<input type="checkbox"/> Yes <input type="checkbox"/> No Legal and Protective Security Data
<input type="checkbox"/> Yes <input type="checkbox"/> No Service History and Case Notes
<input type="checkbox"/> Yes <input type="checkbox"/> No Sensitive Data [AIDS/HIV, Criminal, Abuse, Substance Abuse, Medical and Health]

#### Institution and Service Data:

<b>Overall Settings:</b>
<input type="checkbox"/> Share <b>NO</b> Institution or Service Data [Block All]
<input type="checkbox"/> Share <b>ALL</b> Institution or Service Data [Share Everything]

<b>Override Settings for Institution and Service Data:</b>
<input type="checkbox"/> Yes <input type="checkbox"/> No Allow Users from Another Organization to Place Clients into Services Provided by Your Organization

## ***Information Card and Basic Privacy Script***

### ***BLUE RIDGE HOMELESS MANAGEMENT INFORMATION SYSTEM***

The HMIS is a computer system created to meet a data collection requirement made by Congress to the Department of Housing and Urban Development (HUD). The privacy and safety of those using our services is very important to us. Information gathered about you is personal and private. We collect information needed to provide services, manage our organization, or as required by law.

You will be asked to make two decisions about sharing your information:

1. Whether to allow other participating agencies to see your name, year of birth, and partial social security number.
2. Whether you allow other agencies to see information about other services you have received.

The decision to share is yours and may only be done with your permission. You cannot and will not be denied services that you would otherwise qualify for if you choose not to share information.

Depending on your individual situation, there may be benefits and/or risks for you to carefully consider before you decide whether or not to consent to the release of any identifying information to another agency. You also have the right to request that your name be entered in the system as “anonymous”.

Benefits:

- Coordination of care between agencies that are helping you.
- Reduction in the amount of paperwork that you must do as you seek additional services.
- Better understanding of homeless issues and poverty.

Risks:

- You feel uncomfortable having other agencies see your name or other information.
- You are concerned because you know someone who works for an agency using HMIS.
- There may be physical harm or other negative consequences to you or members of your family if someone found out you sought help, particularly if you or your children have experienced domestic violence, sexual assault, stalking, or child abuse.

Each agency has its own unique sharing plan. Some do not share. With a signed release, some share only general information. Those who share more sensitive case information such as medical, mental health, drug/alcohol or domestic violence may ask you to sign another release.

\_\_\_\_ Yes, tell me more

\_\_\_\_ No

### Your Information Rights

All agencies have a confidentiality policy. The policy follows all US Department of Health and Urban Development (HUD) and Health Insurance Portability and Accountability Act (HIPAA) confidentiality regulations that apply to each participating agency. In general, you have the right to:

- Access your record
- Correct your record
- Refuse to share information including name, year of birth and partial SS#
- Determine the length of time information may be shared
- Withdraw permission to share
- File a grievance, if you believe your confidentiality rights have been violated.

---

Signature

Date

## ***Facts Sheet***

### **FACT Sheet: Blue Ridge Homeless Management Information System (BRHMIS)**

We will enter information you provide to us into a computer program called Homeless Management Information System (HMIS). We are doing this for several reasons:

- To find out what we need to end homelessness in the Roanoke area;
- To provide better service;
- To receive federal funds.
- 

#### **IMPORTANT POINTS ABOUT HOW YOUR INFORMATION WILL BE USED**

- We will use the BRHMIS to keep a record of your contact with our agency.
- We will not share **any** information **without your written permission** through a signed client consent form that allows us to share client profile information with collaborating agencies. This means that you will not have to provide the same information at more than one intake.

#### **HOW WILL MY INFORMATION BE KEPT SECURE?**

We have done several things to make sure that your information is kept safe and secure:

- The computer program we use has the highest security protection available;
- Any information that could identify you, like your name, SS# or birth-date, will be viewed only by people working to provide services to you, and will be removed before reports are issued to local, state, or national agencies;
- All employees agree to follow privacy rules before using the system.

#### **KNOW YOUR RIGHTS**

You have the following rights:

- To review your records within 48 hours.
- To have your record changed so that information is up-to-date and correct.
- To refuse consent and still receive services.
- To file a complaint about how the system was used.

To file a complaint, write to: BRHMIS Steering Committee, in care of the Council of Community Services, P.O. Box 598, Roanoke, VA 24004-0598, Attn: HMIS Administrator.

**(This is a sample site data collection notice, to be posted in accordance with Policy 2-1)**

### *HMIS Data Collection Statement*

We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate.

# BLUE RIDGE HOMELESS MANAGEMENT INFORMATION SYSTEM

## Client Consent for Data Collection

Participation in data collection, although optional, is a critical component of the community's ability to provide the most effective services and housing possible. Please understand that access to shelter and housing services is available without participation in data collection.

This client notice and consent describes how information about you may be used and disclosed and how you can get access to this information. Please review it carefully. If you have any questions or want any further information regarding this form please contact

\_\_\_\_\_ at \_\_\_\_\_.

I, \_\_\_\_\_ (insert client's name), understand and acknowledge that \_\_\_\_\_ (the "Agency") is affiliated with the HMIS, and I consent to and authorize the collection of information and preparation of records pertaining to the services provided to me by the Agency. The information gathered and prepared by the Agency will be included in a Homeless Management Information System ("HMIS") database and shall be used by the Agency to:

- Provide individual case management
- Produce aggregate-level reports regarding use of services
- Track individual program-level outcomes
- Identify unfilled service needs and plan for the provision of new services
- Allocate resources among agencies engaged in the provision of services

\_\_\_\_\_ (please initial) I understand and acknowledge the following collection of information:

(Initial appropriate information)

\_\_\_\_\_ Identifying information (name, birth date, gender, race, social security number, residential information, phone number, family information.)

\_\_\_\_\_ Medical records (except HIV/AIDS and alcohol and drug treatment), psychological records and evaluations, vocational assessment, care coordinators recommendations and direct observations, employment status, etc.

\_\_\_\_\_ Financial information (income verification, public assistance payments and allowances, food stamp allotments)

\_\_\_\_\_ HIV/AIDS diagnosis

\_\_\_\_\_ Substance abuse diagnoses, treatment plan, progress in treatment, discharge.

\_\_\_\_\_ For the specific purpose of: \_\_\_\_\_ further care \_\_\_\_\_ evaluation \_\_\_\_\_ other (please specify other) \_\_\_\_\_

\_\_\_\_\_ (please initial) I understand that I have the right to inspect, copy, and request all records maintained by the Agency relating to the provision of services to me and to receive a paper copy of this form.

\_\_\_\_\_ (please initial) I understand that this release can be revoked by me at any time and that the revocation must be signed and dated by me. I further understand that this consent is subject to revocation at any time, except to the extent that the Agency has already taken action in reliance on it. If not previously revoked, this consent terminates automatically 180 days after my last treatment or discharge from the Agency. I understand that my records are protected by federal, state, and local regulations governing confidentiality of client records and cannot be disclosed without my written consent unless otherwise provided for in the regulations.

Additionally, I understand that participation in data collection is optional, and I am able to access shelter and housing services if I choose not to participate.

DATE: \_\_\_\_\_

SIGNATURE: \_\_\_\_\_

# BLUE RIDGE HOMELESS MANAGEMENT INFORMATION SYSTEM

## Client Consent for Release of Information

CLIENT NAME (first, middle, last): \_\_\_\_\_  
DATE OF BIRTH: \_\_\_\_\_  
SOCIAL SECURITY NUMBER: \_\_\_\_\_ - \_\_\_\_\_ - \_\_\_\_\_

In accordance with Federal Regulation Code 42, Part 2, I hereby authorize:

Homeless Service Organization (check)	To release to/share with:
<input type="checkbox"/> Alleghany County Department of Social Services	_____
<input type="checkbox"/> Blue Ridge Behavioral Healthcare	(Name of individual or institution)
<input type="checkbox"/> Blue Ridge Independent Living Center	_____
<input type="checkbox"/> City of Roanoke Human Services	(Address)
<input type="checkbox"/> Clifton Forge Department of Social Services	_____
<input type="checkbox"/> Council of Community Services	(City, State, Zip code)
<input type="checkbox"/> Covington Department of Social Services	_____
<input type="checkbox"/> RAM House	(Phone/Fax)
<input type="checkbox"/> Roanoke Valley Interfaith Hospitality Network	_____
<input type="checkbox"/> Safe Home Systems, Inc. - Covington	(Email)
<input type="checkbox"/> Salvation Army Red Shield Lodge	_____
<input type="checkbox"/> TAP Transitional Living Center	
<input type="checkbox"/> The Rescue Mission	
<input type="checkbox"/> TRUST House	
<input type="checkbox"/> Veterans Affairs Medical Center	
<input type="checkbox"/> YWCA	
<input type="checkbox"/> Other _____	
(Type in name of organization)	

The following information: (including patient records related to any attempted suicide, emotional illness, psychological services records, if any, social services records, if any; including communications made by me to a social worker, counselor, psychologist, physician, or other health care provider, and information regulated by Federal Public Law 93-282, confidentiality of alcohol and drug abuse patients and records documenting the diagnosis and/or treatment of communicable disease and/or serious disease and infections as defined by the US Department of Health and Human Services rules which include venereal disease, tuberculosis, AIDS, ARC, HIV status and other related diseases, if any)

- Diagnosis/Test Results
- Medical Records/Hospital Records
- Psychological/Psychosocial Assessments
- Substance Abuse Assessments/Evaluations/History
- Psychiatric Evaluation/Consultation/Medications
- Diagnostic Impressions/Prognosis
- Treatment Plan/Treatment Recommendations
- Discharge/Treatment Summary
- Police/Prison Records
- Financial Information
- Housing Requirements
- Transportation Requirements
- Nutritional Requirements
- Chart/Progress Notes

\_\_\_\_ Other (please describe \_\_\_\_\_)

for services covering the dates from: \_\_\_\_\_ to \_\_\_\_\_ for the specific purpose of \_\_\_\_\_ I release the above cited individuals or facilities of any legal liability that may arise from the release of the information requested. I understand that the agency cannot release information obtained from other sources. I understand that the individual/institution/agency receiving this information may not re-release it to any other individual, institution or agency. I also understand that this authorization for release of information will expire on \_\_\_\_\_ unless indicated below.

(not to exceed 365 days)

Condition, date or event of earlier expiration \_\_\_\_\_.

I also understand that this release can be revoked, by me at any time and that the revocation must be signed and dated by me, and that the revoking of the release will not affect information released prior to the revoking of the release.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Relationship (if minor)

\_\_\_\_\_  
Witness Name (PRINT)

\_\_\_\_\_  
Witness Signature

\_\_\_\_\_  
Date

\*\* I hereby revoke my consent for the release of the previously stated information\*\*

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Relationship if Minor

### ***List of Acronyms and Abbreviations***

APR	Annual Progress Report
BRHMIS	Blue Ridge Homeless Management Information System
CCS	Council of Community Services
CoC	Continuum of Care
DSL	Digital Subscriber Line (High-speed internet connection)
FIPS	Federal Information Processing Standards
HIPAA	Health Insurance Portability and Accountability Act of 1996
HUD	U.S. Department of Housing and Urban Development
PA	Partnership Agreement
PA	Participating Agency
PIN	Personal Identification Number
PPI	Protected Personal Information
TA	Technical Assistance

# **List of Revisions, Additions, and Deletions**

Original Issue      December 12, 2007