Blue Ridge Community Assistance Network

Blue Ridge CAN (HMIS) Policies and Procedures

Last Updated October 2015

Blue Ridge Continuum of Care

Council of Community Services – HMIS Lead Agency

Overview and Introduction

These Policies and Procedures were developed to guide the operation of the Blue Ridge Community Assistance Network (Blue Ridge CAN). The Blue Ridge CAN 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 Blue Ridge CAN Steering Committee oversees and guides the development and management of the Blue Ridge CAN. This Blue Ridge CAN Steering Committee is comprised of representatives as appointed by the Continuum of Care (CoC) and participating agencies. Representation should reflect at a minimum a diversity of services represented on the CoC. Through the direction of these dedicated Steering Committee members, these Policies and Procedures reflect the community's stance on the operation of the Blue Ridge CAN. The Council of Community Services is the administrating agency for the Blue Ridge CAN – the Local implementation of HMIS - and the appointed chair convenes the Steering Committee.

The Blue Ridge CAN Steering Committee has as guiding principles that the Blue Ridge CAN:

- 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 Blue Ridge CAN 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 Blue Ridge CAN 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. Blue Ridge CAN staff provides technology, training and technical assistance to users of the system throughout the region.

BENEFITS OF Blue Ridge CAN

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

Homeless Management Information System (HMIS) Data Standards

Following Congressional directive, HUD has supported the development of local Homeless Management Information Systems by: I) providing technical support and funding to CoC's to develop local HMIS; and 2) undertaking a research effort to collect and analyze HMIS data from a representative sample of communities in order to understand the nature and extent of homelessness nationally. As part of this effort, HUD published HMIS Data and Technical Standards (HMIS Standards) in 2004 that allow for the collection of standardized client and program-level data on homeless service usage among programs within a community and across all communities.
The 2004 HMIS Standards ensure that every HMIS captures the information necessary to fulfill HUD reporting requirements while protecting the privacy and informational security of all homeless individuals.

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.

The American Recovery and Reinvestment Act of2009 identified HMIS as the primary tool for the collection of data on the use of funds awarded and persons served through the Homelessness Prevention and Rapid Re-Housing Program (HPRP).
The Data Standards have been further modified to provide the necessary data elements and

guidance to support uniform and consistent tracking of HPRP activities. These modifications were informed through feedback obtained by HUD in February 2009, from homeless assistance providers, Continuum of Care (CoC) representatives, local and state government agency representatives and their associated professional organizations, and homeless advocacy groups. Modifications were also informed by a review of available literature and current practices related to homelessness prevention and rapid re-housing.

Summary of the final revisions to the HMIS Data and Technical Standards
HUD published this document in March 2010.
The Notice adds a new set of Program Description Data Elements.
In addition, the Notice presents revisions to Data Standards for Universal Data Elements and Program-Specific Data Elements. These sections replace Section 2 (Universal Data Elements) and Section 3 (Program-Specific Data Elements) of the 2004 Notice. All other sections of the 2004 notice remain in effect.

The Revised Standards Notice is lengthy and very detailed.
This Summary highlights key changes and compares the final standards to draft standards published in October 2008 and May 2009.
Importantly, the Revised HMIS Data Standards only amend the Data Standards portion of HMIS Technical Standards.
Proposed revisions for HMIS Technical Standards related to privacy, security and other topics will be issued in a subsequent Notice.

HIGHLIGHTS

+The 2009 Notice adds a set of program descriptor data standards-that is, data to be collected about all homeless assistance and HPRP programs in the CoC. The purpose of these new data standards is to ensure that the HMIS is the central repository for all information about homelessness in the CoC, including both programs and clients. These data elements are needed for the following HUD reports:
The Annual Performance Report (APR), the Quarterly Performance Report (QPR) for HPRP funded programs, the Annual Homeless Assessment Report (AHAR) and the Housing Inventory that is submitted as part of the annual CoC application for funding.

+Certain data elements, such as Income and Sources and Non-Cash Benefits, must now be collected at least once annually in addition to being collected at program entry and at exit.

+A follow-up question has been added to data elements that relate to disabilities to determine whether a client is currently receiving services for a condition or received services prior to exiting the program.

+The response categories for "Don't Know" and "Refused" have been added to all relevant data elements to ensure consistency in APR reporting.

+The Reasons for Leaving and Services Received data elements (renamed Services Provided) are no longer required for programs completing APRs. The change for Reasons for Leaving is different than proposed changes in the 2009 Notice.

+There are two new data elements required for street outreach programs that complete APRs. These are: I) a Date of Contact data element that is used to count the number of persons contacted during a program's operating year; and 2) a Date of Engagement data

element that is required to count the number of homeless persons engaged by an outreach program during the operating year.

+The first substantial change between the 2009 draft Standards and the final 2010 Standards relates to a self-sufficiency measure. Programs are NOT required to collect information about clients' progress on one or more domains. That portion of the 2009 draft Standards was not approved.

+The second substantial change between the 2009 draft Standards and the final 2010 Standards relates to definitions of Housing Status, previously called Homeless Status. Housing Status has been added in order to distinguish persons who are literally homeless from those who are at imminent risk of becoming homeless or in a stable housing situation.

The data standards establish uniform definitions for the types of information to be collected and protocols for when data are collected and from whom.

Contributory HMIS Organizations may have additional data collection requirements based on other funding sources, the client population served, and the types of data necessary to effectively monitor programs. These HMIS data element types include Program Descriptor, Universal, and Program-Specific. (Data element types specified in "HUD 2014 HMIS Data Standards Manual – Revised July 2015" available at: ***http://www.councilofcommunitvservices.com/programs/brcan/resources/.***)

Please note that the Privacy or Security Standards Sections from the 2004 Notice are still in effect.

For additional information, refer to:

http://www.councilofcommunitv.services.com/programs/brcan/resources/ for "Homeless Management Information Systems (HMIS); Data and Technical Standards - 2004" and

"HUD 2014 HMIS Data Standards Manual – Revised July 2015" available at: ***http://www.councilofcommunitvservices.com/programs/brcan/resources/.***

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 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 Blue Ridge CAN.

Section 1: Contractual Requirements and Roles

Policy 1-1: Blue Ridge CAN Contract Requirements

The Council of Community Services is committed to coordinate and provide services to Any CoC Agencies 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

- BRCAN-HMIS **General Service Agreement** (pending Attachment l**)** and a
- BRCAN-HMIS **Business Associate Addendum** (or the appropriate Waiver for certain Agencies) (pending Attachment 2)

and comply with the stated requirements.
Agencies will be granted access to the Blue Ridge CAN software system after:

- The BRCAN-HMIS General Service Agreement and BRCAN-HMIS Business Associate Addendum (or the appropriate Waiver for certain Agencies) have been signed with the Council of Community Services, and
- Agencies put into place the stated requirements in the BRCAN-HMIS General Service Agreement.

Agencies agree to comply with the policies and procedures approved by the Blue Ridge CAN Steering Committee.

Policy 1-2: Blue Ridge CAN Steering Committee

A Steering Committee, convened by the Blue Ridge Continuum of Care, representing stakeholders in the HMIS project, will advise all project activities. The committee meets at a minimum of once each quarter. (A current Blue Ridge CAN Steering Committee Membership List may be obtained from the Blue Ridge Continuum of Care).

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

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

Membership of the Blue Ridge CAN Steering Committee will be established according to the following guidelines:

- The Continuum of Care (CoC) will appoint representation that reflects at a minimum a diversity of services represented on the CoC. The Chair of the Steering Committee shall report to the CoC at regularly scheduled meetings.
- The CoC is responsible to find a replacement for any representative that is participating inconsistently or is inactive.
- General membership is drawn from volunteers representing the participating agenc1es.

The Blue Ridge CAN Steering Committee has decision making authority in the following areas:

- Determining the guiding principles that should underlie the implementation activities of the Blue Ridge CAN, including participating organizations, consumer involvement and service programs;
- Selecting the minimal data elements to be collected by all programs participating in the Blue Ridge CAN 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.

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 member has one vote. One designee of the official representative may vote in the absence of the official representative.

Quorum: Half of the committee membership shall constitute a quorum.

Meeting notes: Notes 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 notes as is standard for HUD documentation.

There will be a Data Quality and Evaluation Committee comprised of members selected by the HMIS Steering Committee. This committee will meet as needed and report to the HMIS Steering Committee.

Policy 1-3: Blue Ridge CAN 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 Blue Ridge CAN Steering Committee.
Governance Procedures:

- The Blue Ridge CAN Steering Committee provides recommendations to the Blue Ridge Continuum of Care and the Council of Community Services decisions related to the governance of the Blue Ridge CAN. 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 Blue Ridge CAN Grievance Committee for review.
- The Grievance Committee *(SEE Policy 2-11: Blue Ridge CAN Steering Committee Grievance Procedure)* 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 (HMIS Lead Agency) 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 Leads; and
- Implementing software enhancements recommended by the Blue Ridge CAN 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: Community Assistance Networks (HMIS); Data and Technical Standards Final Notice and all State and Federal regulations as well as to ensure adherence to the Blue Ridge CAN 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 Community Assistance Networks (HMIS); Data and Technical Standards Final Notice and all State and Federal regulations as well as ensuring adherence to the Blue Ridge CAN principles, policies and procedures outlined in this document;
- Is responsible for all activity associated with agency staff access and use of the Blue Ridge CAN data system;
- Is responsible for establishing and monitoring agency procedures that meet the criteria for access to the Blue Ridge CAN 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 Blue Ridge CAN System only to staff who have been trained in the Blue Ridge CAN 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 Blue Ridge CAN 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 Blue Ridge CAN system;
- Ensure organizational adherence to the Blue Ridge CAN 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;

And that the data is entered accurately and on time;

- Provide prompt and timely communications of data, changes in license assignments, and user accounts and software to the Blue Ridge CAN Administrator; and
- Notify immediately the Blue Ridge CAN Administrator of any issue relating to system security or client confidentiality.

Policy 1-5: Participating Agency Lead

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

The Agency Lead will be responsible for duties including:

- Editing and updating agency information;
- Ensuring that access to the Blue Ridge CAN is requested for authorized staff members only after they have:
    a. received training;
    b. satisfactorily demonstrated proficiency in use of the software;
    c. agreed to and signed the User Responsibility Agreement form; and
    d. 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 Blue Ridge CAN 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 Blue Ridge CAN 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 Blue Ridge CAN technical staff and consultants.

The Agency Lead 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;
- Detecting and responding to violations of the Policies and Procedures or Agency procedures.

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

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 Blue Ridge CAN Administrator agrees to authorize use of the Blue Ridge CAN only to users who have received appropriate training, who have completed and signed the BRCAN-HMIS User Responsibility Agreement form (Attachment 3), 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 Blue Ridge CAN responsibilities.
- The Participating Agency agrees to authorize use of the Blue Ridge CAN 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 Blue Ridge CAN 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 Lead and the Blue Ridge CAN 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

Blue Ridge CAN staff will coordinate ongoing training schedules for Agency Leads and End Users. Training will occur on a regular basis. The schedule of trainings will be determined by the Blue Ridge CAN Steering Committee.

Training schedule:

Basic: Introduction to the Blue Ridge CAN System (End User Training)

- Introduction to the Blue Ridge CAN
- Review of applicable policies and procedures
- Confidentiality & Best Practices
- Connecting to the Internet
- Logging on to the Blue Ridge CAN System
- Entering client information including Demographics, Program Enrollments and Services provided, HUD data and Case Management

Program Management: Overview of the Blue Ridge CAN (Agency Lead)

- Review of Agency technical infrastructure including roles and responsibilities
- Review of security policies and procedures
- Review of Blue Ridge CAN technical infrastructure
- Overview of Agency administrative functions
- Assigning User access levels
- Entering and updating information pertaining to the Participating Agency
- Reporting with the Blue Ridge CAN
    - Introduction to reports
    - Using existing reports
    - Creating new reports
    - Exporting information to other software applications

Policy 1-8: Amending Policies and Procedures

The Steering Committee will be responsible for annual review of this document.

Section 2: Participation Requirements

Policy 2-1: Participation and Implementation Requirements

Participation Agreement Requirements

Identification of Agency Lead: Designation of one key staff person to serve as Agency Lead. The Agency Lead 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 Blue Ridge CAN; and

d. Communicating with the Blue Ridge CAN staff about user access and other Blue Ridge CAN activities at the Agency level.

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

Training: Commitment of Agency Lead and designated staff persons to attend training(s) Prior to accessing the Blue Ridge CAN.

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.

Client Data: Agencies must:

a. Obtain signed Data Collection **Acknowledgement** (BRCAN-HMIS Client Acknowledgement & Data Sharing Authorization Form – pending Attachment 4/5) from the client to enter the client's data into the Blue Ridge CAN.

b. Obtain signed **Sharing Authorization** (pending Attachment 4/5) from the client to share personal information with other agencies.

c. Provide written explanation to each client of how information is to be used and stored and on the client's recourse if s/he feels data is misused e.g. grievance policy. Any incident regarding compromise of client confidentiality must be reported to the Blue Ridge CAN 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)**. (See sample in Attachment 8)
While Blue Ridge CAN Policy requires signed **Acknowledgement,** individual Providers may wish to use the following, or similar, 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 needed and appropriate."

Protected Personal Information (PPI) is defined by HUD as "Any information maintained by or for a Covered Homeless Organization (CHO) 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 identity 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 HMIS software development vendor 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 Blue Ridge CAN 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 or other methods to secure computer access to data.

Policy 2-3: Implementation Requirements

For initial implementation, Blue Ridge CAN 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 Blue Ridge CAN staff member who will assist in completion of the Agency's Information Security Protocols.

BRCAN-HMIS Agency General Service Agreement and Business Associate Addendum (pending Attachments 1 & 2):

The Partnership Agreement refers to the document agreement made between the Participating Agency and the Blue Ridge CAN 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.

BRCAN-HMIS User Responsibility Agreement (Attachment 3):

This form is signed by the End Users and Agency Leads to allow them access to the Blue Ridge CAN system. Users must participate in training before given live access to the Blue Ridge CAN system.

Identification of Referral Agencies:
The Blue Ridge CAN will develop processes to track referrals to Blue Ridge CAN Participating Agencies, as well as Agencies not participating in the Blue Ridge CAN (Referral-only or Non-member Agencies).
(SEE pending Attachment 6: "BRCAN-HMIS **"REFERRAL ONLY" AGENCY Request Form.**")

Participating agency referrals are tracked in the Blue Ridge CAN: clients are "placed" into local agency services or **referred** to another agency's services.

These Referrals are tracked by Services Reports, which include Actual Services, as well as Service Referral to Agencies which provide those Services.

Policy 2-4: Interagency Data Sharing Agreements

Responsibilities:

Each Agency is responsible for the initiation, negotiation, and completion of Interagency Data Sharing Agreements (Attachment in Development) 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 Blue Ridge CAN System Administrator (HMIS Coordinator) 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 Blue Ridge CAN System will provide, in writing, an agreement that has been signed between the Executive Directors of Participating Agencies. Completed agreements will be presented to Blue Ridge CAN for review and archival.

- See Interagency Sharing Agreement (Attachment 5).
- 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 Blue Ridge CAN 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 Blue Ridge CAN.
- 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 – Informed Consent

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

Each **Participating Agency (PA)** must publish the Blue Ridge CAN privacy notice describing policies 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 Blue Ridge CAN 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 Blue Ridge CAN only if the use or disclosure is allowed by the HUD HMIS Final Notice, and is described in this privacy notice. HIPAA regulations receive precedence over the HUD Final Notice PPI policies.** Blue Ridge CAN 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 Blue Ridge CAN 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 **P**A 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: (I) 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 Blue Ridge CAN. The Participating Agency will provide an oral explanation of the Blue Ridge CAN 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:

1. What the Blue Ridge CAN 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
   - To help their clients receive the assistance they need most efficiently
   - 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 relevant 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 Blue Ridge CAN database.
   - Client has the right to know who has added to, deleted, or edited their Blue Ridge CAN electronic client record
   - Information transferred over the web is 128-bit encrypted (SSL)

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 and signed Consent:

Signed Acknowledgement to Enter Data:

Each client must provide written acknowledgement that they have been informed that their data will be entered into the BRCAN.

Signed Authorization 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 (Attachment 5).

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, unless required by State or Federal Law.

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 (UDE)

The universal data elements **include**: Name, Social Security Number, Date of Birth, Race, Ethnicity, Gender, Veteran Status, Disabling Condition, Resident Prior to Program Entry, Zip Code of Last Permanent Address, Housing Status, Program Entry Date, Program Exit Date, Personal Identification Number, and Household Identification Number.

More information on the UDE to be collected is available in the "HUD 2014 HMIS Data Standards Manual – Revised July 2015" available at: ***http://www.councilofcommunityservices.com/programs/brcan/resources/.***

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 Anti-Virus/Spy/Malware 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 vender.
- 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. Blue Ridge CAN 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 Blue Ridge CAN 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 Blue Ridge CAN.
2. Backup: While the Blue Ridge CAN 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 Blue Ridge CAN. 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: Blue Ridge CAN Steering Committee Grievance Procedure

The Blue Ridge CAN Steering Committee holds the final authority for all decisions related to the governance of the Blue Ridge CAN System. Decisions made or actions authorized by Blue Ridge Regional Continuum Of Care regarding the Blue Ridge CAN which do not satisfy an interested party, including those at the Continuum, Agency or Client levels, may be brought before the Blue Ridge CAN Grievance Committee for a decision in Accordance with the Blue Ridge CAN 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, and three Steering Committee members. If conflict with committee member exists, one CoC representative will be appointed by the Committee Chair.

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 Blue Ridge CAN, as these issues are most likely within a Participating Agency.

It is only when the issue involves the actions of the Blue Ridge CAN regional operation that the Blue Ridge CAN's Grievance Procedure is to be used. Additionally, the Blue Ridge CAN Grievance Procedure is not intended for use as an "appeal" for a local agency decision.

If a client wants to file a grievance:

1. The Client grievance 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 grievance is to be stated in writing.
3. The grievance shall be returned to the Blue Ridge CAN party who has the ability and authority to take corrective action. If needed, the Blue Ridge CAN 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 Blue Ridge CAN party to resolve the grievance.
5. The actions and resolutions shall be in writing.
6. If the matter cannot be resolved to the satisfaction of all parties, the Blue Ridge

CAN 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 grievance.
8. The Grievance Committee will resolve the grievance within five (5) working days after meeting.
9. Should the client want to appeal the Grievance Committee's decision, the Blue Ridge CAN Steering Committee will hear the grievance at its next scheduled meeting and resolve the grievance 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 Blue Ridge CAN party involved will have a copy describing the resolution of the Grievance.

Grievance by Participating Agencies or a Continuum of Care:

Participating Agencies who are participating in the Blue Ridge CAN 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 grievance about a decision or an action of the Blue Ridge CAN staff concerning the Blue Ridge CAN or any issue about which the Blue Ridge CAN has responsibility, they should first bring the matter to the attention of the Blue Ridge CAN System Administrator or designee and/or the party who has the ability and authority to take appropriate corrective action as a verbal, informal Grievance Procedure.

Informal Grievance Procedure:

The informal grievance procedure involves bringing the issue verbally to the Blue Ridge CAN party who has the ability and authority to take corrective action (i.e. HMIS Coordinator). 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 grievance should be in writing and submitted to the Blue Ridge CAN Steering Committee who will convene the Grievance Committee. (SEE Attachment 7: "Grievance Appeal Form")
2. The Grievance Committee will meet no later than ten (10) working days after being convened and notified of the grievance and will consider information from all parties involved.

3. The Grievance Committee will hear the grievance from all parties.
4. The Grievance Committee will resolve the grievance 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 Blue Ridge CAN Steering Committee, who will hear and resolve the grievance 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 Blue Ridge CAN System Administrator.

Designation of User Levels: There are different levels of access to the Blue Ridge CAN. 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 complete and sign (upon hire, and when modified) a BRCAN-HMIS User Responsibility Agreement form- as provided in Section *Policy 2-3: Implementation Requirements- BRCAN-HMIS User Responsibility Agreement (Attachment 3),* and 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 Blue Ridge CAN 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 (PPI) that is either generated by or for the Blue Ridge CAN, including, but not limited to reports, data entry forms and signed consent forms.

All paper or other hard copy generated by or for the Blue Ridge CAN 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 Blue Ridge CAN paper records that contain client information must be maintained in accordance with Agency guidelines.

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 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** (contain at least one number).
- 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 and issued to the User by the Blue Ridge CAN System Administrator. The first time temporary password can be communicated via e-mail, telephone or in person. The System Administrator will reset a password if necessary. Only temporary passwords will be sent via e-mail, and must be changed as immediately as possible by the User.
- 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 an email request is provided by that user to the Blue Ridge CAN System Administrator.

All User accounts will be the responsibility of the Blue Ridge CAN System 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 Blue Ridge CAN System 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 Blue Ridge CAN System Administrator. If access is restricted, the Blue Ridge CAN System Administrator will notify the Chair of the Steering Committee and the CoC Chair 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 CAN Steering Committee.
6. Privileges may be reinstated by Blue Ridge CAN Steering Committee review.

Policy 3-6: Data Access Control

Agency Leads at Participating Agencies and Blue Ridge CAN System Administrator reserve the right to monitor access to system software.

- Agency Leads at Participating Agencies and Blue Ridge CAN System Administrator will regularly review User access privileges and deactivate users when users no longer require access.
- Agency Leads at Participating Agencies and Blue Ridge CAN System Administrator may implement discretionary access controls to limit access to Blue Ridge CAN

information based on application security designations. Examples of such designations include but are not limited to "Agency Lead", "Case Manager", and "Volunteer".

- Participating Agencies and Blue Ridge CAN System Administrator may audit unauthorized accesses and attempts to access Blue Ridge CAN information.
- Audit records shall be kept at least six months, and Agency Leads and the Blue Ridge CAN System 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 Computers that are used to collect and store HMIS 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.
- Each User should have a unique identification code.
- Each User's identity should be authenticated through an approved 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** (90) 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 Blue Ridge CAN Data for Research

Agencies participating in the Blue Ridge CAN 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 (PPI) 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 provided

d. to operate the agency, including administrative functions such as legal, audits, personnel, oversight, and management functions

e. to comply with reporting obligations

f. when required by law

g. for research purposes

Blue Ridge CAN 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 Blue Ridge CAN Steering Committee prior to publication, for publication approval by the Blue Ridge CAN Steering Committee.
- Research will be shared with the appropriate agencies after publication.
- Blue Ridge CAN Steering Committee will be granted the rights to utilize all findings (results).

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

Section 4: Technical Support and Staff Availability

Policy 4-1: Planned Technical Support

The Blue Ridge CAN System Administrator, in conjunction with Agency Lead 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 Blue Ridge CAN 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 Blue Ridge CAN staff have been developed:

- Service request from participating agency
  1. End user informs Agency management staff (Executive Director/designee or Agency Lead) of the problem.
  2. Agency management staff attempts to resolve the issue. If unable to resolve, Agency staff may contact Blue Ridge CAN staff directly in order to request expedited service.
  3. Blue Ridge CAN staff determines resources needed for service and if necessary, contacts the Blue Ridge CAN Administrator or vendor for support.
  4. Blue Ridge CAN staff contacts Agency management staff to work out a mutually convenient service schedule and resolution to the 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- Blue Ridge CAN Staff >>
  4- Blue Ridge CAN System Administrator and/or

  HMIS Vendor (Currently [2015] Pathways, Bowman as of February 1, 2016)

Policy 4-3: Blue Ridge CAN Staff Availability

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

Section 5: Stages of Implementation

Policy 5-1: Stage 1. Planning

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

I. Completed security assessment, including all participation and data sharing agreements as well as client consent protocols;

2. Identified their Agency's Blue Ridge CAN Agency Lead; and

3. Made proper connectivity arrangements as per Blue Ridge CAN administrator.

During Stage I of implementation of the Blue Ridge CAN:

1. Participating Agency staff and Blue Ridge CAN staff meet for the Security Assessment meeting.

2. Blue Ridge CAN staff and Agency Lead 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 Blue Ridge CAN System Administrator.

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

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

Activities during Stage 2 of implementation:

- Blue Ridge CAN System Administrator creates user IDs and temporary passwords for all users.
- Site Users and the Agency Lead receive training on uses of the Blue Ridge CAN HMIS.
- Trained agency staff work to enter client data into the system using the processes taught during training. These may be different for HOD-funded agencies and non-HOD-funded agencies.

The Blue Ridge CAN Stage 2 continues until data has been entered on I00% 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 Enrolled in 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 I00% of clients served or for an entire month on all clients served.

Stage 3 of implementation:

- Begins when staff utilizes the Blue Ridge CAN System to maintain client records, including applicable Program and 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 Blue Ridge CAN staff to complete all stages. To ensure that all parties are comfortable with the process and progress for this stage, the Participating Agency and Blue Ridge CAN staff may meet again to assess if obstacles to progress exist.

Section 6: Attachments

Attachment 1: *BRCAN-HMIS General Service Agreement*

Attachment 2: *BRCAN-HMIS Business Associate Addendum*

Attachment 3*: BRCAN-HMIS User Responsibility Form*

Attachment 4: *BRCAN-HMIS Client Acknowledgement & Data Sharing Authorization Form*

Attachment 5: *"Referral Only" Agency Request Form*

Attachment 6: *Grievance Appeal Form*

Attachment 7: *Sample Site Data Collection Notice*

Attachment 8: *Family Consent Form*

Attachment 9: *BRCAN-HMIS Notice of Privacy Practices Certification*

Attachment 10: *BRCAN-HMIS Client Opt-Out Form*

Attachment 11: *User Policy for Blue Ridge CAN*

Blue Ridge Community Assistance Network (BRCAN – HMIS) Local HMIS Agency General Service Agreement – current example (ignore minor discrepancies)

This General Service Agreement (the "Agreement") is entered into between BRCAN-HMIS Community Network, Inc. ("BRCAN-HMIS"), The Council of Community Services (CCS) - "VA-502 Blue Ridge CoC" ("HMIS Lead Agency") and _____, ("Agency") (each, a "Party" and collectively, the "Parties") on _____, 20xx (hereinafter, the "Effective Date").

1. AGENCY REQUIREMENTS

(a) The Agency will:

- ./ Designate one or more of its Personnel (as defined below) who will be trained to access and supplement client records on BRCAN-HMIS Systems (as defined below)
- ./ Designate one staff person to accept and process all BRCAN-HMIS related grievance procedures (the "Grievance Officer')
- V' Maintain an up-to-date list of all such designated persons, and supply it to the BRCAN-HMIS Community Network. Any changes in these lists must be immediately reported to BRCAN-HMIS Community Network
- V' Develop an Agency privacy policy and post a Privacy notice at the service location

(b) The Agency agrees to use due diligence and care in assigning employees, independent contractors, and volunteers (hereafter, "Personnel") to use the BRCAN-HMIS Systems. For purposes of this paragraph, "due diligence" means that the Agency shall ensure that only those Agency Personnel will be permitted access to BRCAN-HMIS Systems by Agency who have completed (to Pathway's reasonable satisfaction) introductory and ongoing confidentiality and ethics training provided by BRCAN-HMIS (as set forth in Section 5 hereof), who have satisfied all of Agency's credentialing criteria (which are consistent with applicable industry standards), and who conform to Pathway's requirements that prohibit the sharing of password or access codes. Agency will not permit any Agency Personnel who do not satisfy the foregoing requirements to have any access to BRCAN-HMIS Systems (hereafter, "Unauthorized Persons").

(c) For purposes of this Agreement, "BRCAN-HMIS Systems" means BRCAN-HMIS COMPASS and BRCAN-HMIS' proprietary, Internet-based programs and tools that are part or components thereof.

(d) The Agency agrees to meet or exceed organizational security standards contained in the U.S. Department of Housing and Urban Development's (such agency referred to hereafter as "HUD) HMIS Data and Technical Standards, published in Federal Register volume 69 number 146 on July 30, 2004. The complete standards and official guidance on their implementation can be found at www.hmis.info

(e) Agency warrants that the "Data") required under the standard policy and operating procedure manual of HMIS Lead Agency (the "HMIS Policy and Procedures Manual") is accurate, complete and in compliance with such HMIS Policy and Procedures Manual as well as any local Continuum of Care policies.

2. AUDITS

BRCAN-HMIS and the HMIS Lead Agency reserve the right to inspect activity on the BRCAN-HMIS Systems to ensure proper utilization and safe practices. Upon determining that Agency fails to comply with system policies and procedures or the provisions of Sections 1(b), 3, 4, and 5 hereof, and the BRCAN-HMIS Business Associate Agreement, BRCAN-HMIS will immediately deny Agency access to BRCAN-HMIS Systems.

3. CONFIDENTIALITY

All client information contained in or transmitted via BRCAN-HMIS Systems will be confidential. The Agency agrees to abide by all present and future federal, state and local laws and regulations regarding confidentiality of client records contained in or transmitted via BRCAN-HMIS Systems.

4. ACCESS TO DATA

The Agency agrees to limit access to information in the BRCAN-HMIS Systems to Agency Personnel in accordance with Section 1. Without limiting the generality of the foregoing, the Agency shall ensure that only Agency Personnel who satisfy the requirements of Section 1 shall be permitted access to information in the BRCAN-HMIS Systems for the purpose of:

- !/' Verifying eligibility for services
- !/' Creating and updating case plans
- *V* Keeping records of services provided
- !/' Generating statistical analysis of services and their effectiveness

The Agency will use best efforts, consistent with applicable industry standards, to prevent Unauthorized Persons from accessing BRCAN-HMIS Systems. Without limiting the generality of the foregoing, Agency shall ensure that it has policies and procedures in place to prevent any such unauthorized access. The Agency shall permit BRCAN-HMIS, the HMIS Lead Agency and a representative of the local Continuum of Care lead agency as defined by HUD (the "Local Continuum of Care Representative") to review such policies and procedures upon request.

The Agency grants the BRCAN-HMIS and the HMIS Lead Agency permission to access and utilize Data for the sole purposes of system administration, technical support, auditing, research, and compliance with applicable legal and regulatory requirements and satisfying its obligations under this Agreement. BRCAN-HMIS and the HMIS Lead Agency agree not to further disclose personally identifiable information of Agency's clients on the BRCAN-HMIS system other than as permitted or required by this Agreement, the BRCAN-HMIS Business Associate Agreement, or as required by law.

The Local Continuum of Care Representative may also have access to HMIS data within their Continuum of Care for purposes of reporting and monitoring for HUD-designated Continuum of Care requirements. The representative and their designees will follow all security and privacy policies and will complete all Confidentiality and Ethics training.

From time to time, the HMIS Lead Agency, the Local Continuum of Care Representative, or BRCAN-HMIS (with authorization from the Lead Agency or Continuum of Care) may provide aggregate data to (a) agencies affiliated with VA-502 Roanoke Valley HMIS so that such agencies may compare their experience with other agencies reporting data in VA-502 Roanoke Valley HMIS, b) researchers, c) government entities, d) funders. No individually identifiable data will be released with respect to such aggregation of data without prior authorization by the individual to whom such information pertains or without other Wise being done in compliance with applicable laws and regulations. No agency-identifying information (i.e., identifying agency or its Data) will be released without the written authorization of the applicable agency.

BRCAN-HMIS agrees not to provide access to any agency or client level data to any parties outside of those listed above without the written permission of the Agency.

5. STAFF VOLUNTEER REQUIREMENTS

Agency Personnel who enter or review client information must first participate in an introductory training session conducted by BRCAN-HMIS staff or by an employee of Agency who has been certified by BRCAN-HMIS to conduct such training. Agency Personnel who enter or review client records must also attend periodic confidentiality and ethics "best practices" training, conducted by BRCAN-HMIS staff or consultants retained by BRCAN-HMIS. Staff, volunteers or other Agency Personnel who have not attended this training shall not access the BRCAN-HMIS Systems.

No Agency Personnel may *enter* information regarding an individual client in BRCAN-HMIS Systems unless Agency has first obtained a signed client authorization form approved by BRCAN-HMIS (the "Client Authorization Form") from the client, or unless a Client Authorization Form previously signed by the client, and currently in effect, is on file at the Agency. The Agency shall keep these signed forms on file, and must make them available for audit by BRCAN-HMIS upon request.

No Agency Personnel may *view* information regarding an individual client in BRCAN-HMIS Systems unless Agency has first obtained a signed Client Authorization Form from the client, or that a Client Authorization Form previously signed by the client, and currently in force, is on file at the Agency. The Agency must keep these signed forms on file, and must make them available for audit by BRCAN-HMIS staff upon request.

6. DISPUTED INFORMATION

Agency shall maintain an internal appeals process regarding client grievances. In the event that a client disputes information in BRCAN-HMIS Systems that was entered into by Agency Personnel:

The client will be referred to Agency, who's Grievance Officer will make a good-faith effort to resolve the issue. If the client is not satisfied with the Grievance Officer's response, Agency shall permit the client to appeal the response using Agency's internal appeals process and shall inform the client how to do so.

If the result obtained by the Grievance Officer or through the internal appeals process indicates that the information entered by Agency Personnel should be changed, Agency shall ensure that such change is made. Upon Agency's request, BRCAN-HMIS will provide reasonable assistance in amending the affected client record.

7. OWNERSHIP

a. Agency's Ownership of Data. Data that Agency's Personnel input into BRCAN-HMIS Systems remain the sole property of the Agency.

b. BRCAN-HMIS' Ownership of BRCAN-HMIS Systems. BRCAN-HMIS Systems, and any improvements, modifications, enhancements, customizations, changes, updates, and versions thereof and compilations and derivatives thereof, prepared or provided by BRCAN-HMIS, Agency, HMIS Lead Agency, or any other party, and all copies thereof, whether created or developed prior to, during, or after the term of this Agreement, and all intellectual property related to or embodied in any of the foregoing (collectively, the "BRCAN-HMIS' Intellectual Property") are proprietary to and, as to BRCAN-HMIS, Agency, and HMIS Lead Agency, belong exclusively to BRCAN-HMIS, and title to them shall remain at all times with BRCAN-HMIS. To the extent that Agency, HMIS Lead Agency, or any of their respective Personnel, retains or acquires any right, title, or interest in any BRCAN-HMIS' Intellectual Property, Agency and HMIS Lead Agency hereby irrevocably assign, and shall use best efforts to ensure that their respective Personnel irrevocably assign, all right, title, and interest in and to BRCAN-HMIS' Intellectual Property to BRCAN-HMIS. Agency and HMIS Lead Agency further agree to, and shall ensure that their respective Personnel shall agree to, execute all further documentation and provide all assistance reasonably necessary to achieve the intent of this Section. Agency and HMIS Lead Agency each agree that this Agreement contains no right in or license to any source code contained in or related to BRCAN-HMIS Systems. Neither Agency nor HMIS Lead Agency shall sell, transfer, publish, disclose, display, or otherwise permit or otherwise make available to any other persons or entities the BRCAN-HMIS' Intellectual Property except as expressly allowed under this Agreement. All rights and title in the BRCAN-HMIS Systems and any other BRCAN-HMIS' Intellectual Property not expressly granted to Agency or HMIS Lead Agency hereunder are reserved by BRCAN-HMIS. Any contrary provision herein notwithstanding, the foregoing provisions of this Section 7 are, as between BRCAN-HMIS and HMIS Lead Agency, subject to Section Four, L of that certain HMIS Agreement between BRCAN-HMIS and HMIS Lead Agency dated July 1, 2009 as applicable.

8. WARRANTY DISCLAIMER AND LIMITATION OF LIABILITY

a. BRCAN-HMIS MAKES NO WARRANTIES, INCLUDING, WITHOUT LIMITATION, WITH RESPECT TO THE BRCAN-HMIS SYSTEMS, BRCAN-HMIS' SERVICES, HARDWARE, OPERATIONAL SOFTWARE OR ANY THIRD PARTY SOFTWARE, WHETHER EXPRESS OR IMPLIED, ORAL OR IN WRITING, IN FACT OR ARISING BY OPERATION OF LAW, COURSE OF DEALING, USAGE OF TRADE, OR OTHERWISE, AND DISCLAIMS ANY LIABILITY IN CONNECTION WITH ANY SUCH WARRANTIES, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR INFRINGEMENT, AND ALL SUCH WARRANTIES ARE EXPRESSLY AND SPECIFICALLY DISCLAIMED. BRCAN-HMIS MAKES NO REPRESENTATIONS OR WARRANTIES THAT USE OF THE BRCAN-HMIS SYSTEMS WILL BE UNINTERRUPTED OR ERROR-FREE. BRCAN-HMIS MAKES NO WARRANTY AND DISCLAIMS ANY LIABILITY REGARDING THE VALIDITY OF ANY DATA AND/OR INFORMATION THAT IS ENTERRED INTO THE BRCAN-HMIS SYSTEMS BY ITS USERS (INCLUDING AGENCY), AND BRCAN-HMIS SHALL NOT BE RESPONSIBLE FOR ANY INACCURATE DATA OR INFORMATION THAT IS GENERATED BY THE BRCAN-HMIS SYSTEMS DUE TO INACCURATE DATA OR INFORMATION THAT IS ENTERED INTO THE BRCAN-HMIS SYSTEMS BY ITS USERS (INCLUDING AGENCY). IN NO EVENT SHALL BRCAN-HMIS BE LIABLE TO AGENCY, HMIS LEAD AGENCY, OR ANY THIRD PARTY FOR ANY CLAIM, LOSSES, OR DAMAGES ARISING FROM RELIANCE ON ANY DATA OR INFORMATION AVAILABLE ON OR OBTAINED THROUGH USE OF BRCAN-HMIS SYSTEMS.

b. BRCAN-HMIS and the HMIS Lead Agency shall not be liable to Agency, and BRCAN-HMIS shall not be liable to HMIS Lead Agency, under any legal theory (including, without limitation, negligence) for any direct, indirect, special, incidental, consequential, or similar damages (including, without limitation, lost revenues) in connection with BRCAN-HMIS Systems. In no event shall BRCAN-HMIS be liable to Agency or HMIS Lead Agency for damages in an amount equal to more than the total amount of payments made by Agency to BRCAN-HMIS under this Agreement.

9. TERM OF AGREEMENT

Subject to the provisions of Section 11 hereunder, this Agreement shall commence on the Effective Date and continue in full force and effect for an initial term of one (1) year and shall automatically renew for successive one-year periods thereafter.

10. TERMINATION

Any Party may terminate this Agreement upon thirty (30) days prior written notice to the other Parties. Notwithstanding the foregoing, access to BRCAN-HMIS Systems and services may be interrupted or terminated if payment of the annual participation fee is not received as agreed upon, or if the Agency fails to comply with the provisions set forth under Sections 1, 2, 3, 4, or 5 of the Agreement.

11. ENTIRE AGREEMENT

This Agreement, all schedules and attachments thereto, and the BRCAN-HMIS Business Associate Agreement set forth the entire agreement and understanding among the Parties relating to the subject matter contained herein and therein and supersede all other prior oral or written agreements heretofore made among the Parties. Any amendment hereto must be

in writing and signed by all Parties. This Agreement may be executed in multiple counterparts, but all such counterparts shall be considered one and the same document.

This Agreement is not valid unless accompanied by a fully executed BRCAN-HMIS General Service Agreement and a fully executed BRCAN-HMIS Business Associate Agreement.

12. Authorization. Each of the Parties has been authorized by its board of directors and/or executive committee to enter into this Agreement.

13. Agency has attached the following documents to this agreement:

BRCAN-HMIS General Service Agreement

BRCAN-HMIS Business Associate Addendum

o Other: _____

14. Notices. Any notice required or permitted to be given under this Agreement must be in writing and (i) sent by certified mail, return receipt requested, and will be deemed given 3 days after the date of postmark, or (ii) by national delivery service (such as Federal Express, UPS, or DHL) and will be deemed given upon confirmation of delivery by such delivery service provider. Notice shall be addressed to the Parties' mailing addresses stated below on the signature page of this Agreement unless changed by notice given in accordance with this provision.

15. NO THIRD-PARTY BENEFICIARIES. None of the provisions of this Agreement shall be for the benefit of, or enforceable by, any party other than a Party hereto.

16. WAIVER. No waiver of any breach of the Agreement shall constitute a waiver of a subsequent breach.

17. SEVERABILITY. If any provision of this Agreement is held invalid or unenforceable by a court or agency of competent jurisdiction, the remaining provisions shall nevertheless remain valid and shall continue in full force and effect.

18. SURVIVAL. All rights and obligations of the Parties that have accrued through operation of this Agreement shall survive its termination or expiration, along with all provisions that by their terms survive and those which must survive to give effect to their terms. Without limiting the generality of the foregoing, Sections 3, 4, 7, 8, 9, this Section 19, and Section 20 shall survive termination or expiration of this Agreement.

19. CHOICE OF LAW. This Agreement shall be governed and construed under the laws of the State of Georgia, without regard to its conflicts-of-law principles.

20. APPLICABILITY TO HMIS LEAD AGENCY AND LOCAL CONTINUUM OF CARE REPRESENTATIVE. To the extent that HMIS Lead Agency, Local Continuum of Care Representative, or their respective Personnel shall access the BRCAN-HMIS Systems or data or information maintained thereon, the use and access restrictions and confidentiality requirements that apply to Agency pursuant to the terms and conditions of this Agreement, including but not limited to those set forth at Sections 1(b), 3, 4, and 5 of this Agreement, shall apply with equal force to HMIS Lead Agency and Local Continuum of Care Representative, to the extent applicable to the activities of HMIS Lead Agency and/or Local Continuum of Care Representative resulting in, requiring, or giving rise to such access.

[Executions on next page.]

IN WITNESS WHEREOF, the parties have entered into this Agreement effective as of the Effective Date.

By: _____

Name: _____

Local HMIS Agency Name:

_____

Address:

_____

City: _____ State: ___ Zip: ___

Attest: ----------

Date: _____

By: ----------

_____, Executive Director
Blue Ridge CAN / HMIS Vendor Entity

Attest: ----------

Date: _____

By: _____

Name: _____

Agency: _____

Covering: "VA-502 - Blue Ridge CoC"

Address: _____

City: _____ State: ___ Zip: ___

Attest: _____

Date: _____

Acknowledged and agreed: I have read and understand the Agreement and agree to comply with its terms.

Local Continuum of Care Representative:

By: _____

Print Name: _____

Attest: _____

Date: _____

Blue Ridge Community Assistance Network (BRCAN – HMIS) Local HMIS Agency General Service Agreement – current example (ignore minor discrepancies)

BUSINESS ASSOCIATE ADDENDUM

This Business Associate Addendum (the "Addendum"), is entered into between BRCAN-HMIS Community Network, Inc. ("BRCAN-HMIS"), The Council of Community Services (CCS) - "VA-502 Blue Ridge CoC" ("HMIS Lead Agency") and _____, ("Agency") (each, a "Party" and collectively, the "Parties") on _____, 20xx (hereinafter, the "Effective Date").

RECITALS

WHEREAS, the Parties have entered into a General Service Agreement dated effective as of the Effective Date (the "Agreement") to which this Addendum is appended;

WHEREAS, under the terms of the Agreement, the Covered Entity may provide, and the Business Associate may have access to. certain information, some of which may constitute Protected Health Information ("PHI");

WHEREAS, the Covered Entity desires to obtain satisfactory assurances that the provision of such information complies fully with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and any regulations adopted pursuant to HIPAA and the regulations adopted at 45 C.F.R. § 164.504(e); and

WHEREAS, the Parties desire to append the Agreement to ensure that the provision of any PHI to Business Associate conforms with the business associate requirements established pursuant to HIPAA and the regulations adopted at 45 C.F.R. § 164.504(e);

NOW, THEREFORE, in consideration of the mutual promises of the Parties hereto, and of the mutual covenants and conditions hereinafter set forth, the Parties agree as follows:

I. Definitions.

A. *Breach of Unsecured Protected Health Information:* shall have the meaning set forth in 45 C.F.R. § 164.402, and, with respect to such information, the term "Breach" shall have the meaning also set forth therein.

B. *Covered Entity:* shall have the meaning set out in its definition at 45 C.F.R. § 160.103, as such provision is currently drafted and as it is subsequently updated, amended or revised. For purposes of this Addendum, _____ shall be considered the Covered Entity.

C. *Designated Record Set:* shall have the meaning as set out in its definition at 45 C.F.R. § 164.501, as such provision is currently drafted and as it is subsequently updated, amended or revised.

D. *Health Care Operations:* shall have the meaning set out in its definition at 45 C.P.R. § 164.501, as such provision is currently drafted and as it is subsequently updated, amended or revised.

E. *HITECH Act:* shall mean the Health Information Technology for Economic and Clinical Health Act of2009. F.

Individual: shall have the meaning set out in its definition at 45 C.P.R. § 164.501, as such provision is currently drafted and as it is subsequently updated, amended or revised, and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

G. *Individually identifiable health information:* shall have the meaning set out in its definition at 45 C.P.R. § 164.103, as such provision is currently drafted and as it is subsequently updated, amended or revised.

H. *Privacy Rule:* shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.

I. *Protected Health information* ("PHI"): shall have the meaning set out in its definition at 45 C.F.R. § 164.501, as such provision is currently drafted and as it is subsequently updated, amended or revised, and for purposes of this Addendum shall be limited to infonnation created or received by Business Associate from or on behalf of Covered Entity.

J. *Security Rule:* shall mean the Security Standards for the Protection of Electronic Protected Health Infonnation at 45 C.F.R. Part i64, Subpart C.

2. Limits on Use and Disclosure of PHI.

Except as otherwise specified herein, Business Associate may use and disclose PHI only as necessary to perform its obligations under the tenns of the Agreement. All other uses and disclosures not specifically authorized by the Agreement, this Addendum, or applicable state or federal law are strictly prohibited.

3. Business Associate's Obligations.

With regard to its use or disclosure of PHI, Business Associate shall:

A. Not use or further disclose PHI other than as pennitted or required by this Addendum or as required by law;

B. Use reasonable and appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by this Addendum. Business Associate will also implement, Administrative, Physical, and Technical Safeguards (each as defined at 45 C.F.R. § i64.304) to protect the confidentiality. availability, and integrity (as defined at 45 C.F.R. § i64.304) of any PHi that Business Associate creates, receives, maintains, or transmits on behalf of the Covered Entity. Business Associate agrees to mitigate, to the extent practicable, any harmful effects that are known to Business Associate of a use or disclosure of PHI in violation of the requirements of this Addendum. Pursuant to Sections 13401(a) and 13404(a) of the HITECH Act, and commencing on the applicable effective date thereunder, the additional requirements thereof that relate to security and privacy and that are made applicable thereunder to Covered Entity shall also apply to Business Associate with respect to PHI, which requirements applicable to Business Associate with respect to PHI are, effective as of such effective date, incorporated herein by this reference in accordance with the HITECH Act;

C. Provide notice to Covered Entity of any use and/or disclosure of PHI that is not permitted or required by this Addendum within ten (10) days of Business Associate becoming aware of such use and/or disclosure. Business Associate also agrees to immediately notify Covered Entity of any Security Incident (as defined at 45 C.F.R. § 164.304) involving PHI upon Business Associate having knowledge of same. Following the discovery by Business Associate of a Breach of Unsecured Protected Health Information affecting PHI, Business Associate shall notify Covered Entity thereof as required by and in accordance with 45 C.F.R. § i64.4l0;

D. Enter into written agreements with any and all agents and subcontractors, to whom it provides PHI (including any electronic PHI) received from, or created or received by Business Associate on behalf of, Covered Entity pursuant to which written agreements such agents and subcontractors shall agree to adhere to the same restrictions and conditions on the use or disclosure of PHI that apply to Business Associate pursuant to this Addendum;

E. Make available PHI maintained in Designated Record Sets to Covered Entity, at Covered Entity's request and in the time and manner reasonably designated by Business Associate, in accordance with 45 C.F.R. § 164.524;

F. Make PHI available to Covered Entity, at Covered Entity's request and in the time and manner reasonably designated by Business Associate, for purposes of amendment and to incorporate any such amendments to the PHI in accordance with 45 C.F.R. § i64.526;

G. Make information available to Covered Entity, at Covered Entity's request and in the time and manner reasonably designated by Business Associate, to provide an accounting of the disclosures of PHI made in accordance with 45 C.F.R. §i64.528;

H. Make available its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity to the Secretary of The Department of Health and Human Services, in the time and manner designated by said Secretary, for purposes of determining Covered Entity's compliance with the Privacy Rule;

I. Notify Covered Entity within five (5) days of Business Associate's receipt of any request or subpoena for PHI. To the extent that Covered Entity decides to assume responsibility for challenging the validity of such request or subpoena, Business Associate shall reasonably cooperate with Covered Entity in such challenge, at Covered Entity's sole cost and expense;

1. To the extent required by the "minimum necessary" requirements of the Privacy Rule, only request, use, and disclose the minimum necessary amounts of PHI necessary to accomplish the purpose of the request, use, or disclosure; and

K. Upon termination of the Agreement, if feasible, return to Covered Entity or destroy, all PHI received from, or created or received by Business Associate on behalf of, Covered Entity that Business Associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of this Addendum to the PHI and limit further use or disclosure to those purposes that make the return or destruction of such information infeasible.

4. Business Associate's Activities.

Except as otherwise specified in this Addendum, Business Associate may:

A Use PHI in its possession for its proper management and administration and to fulfill any present or future legal responsibilities of Business Associate provided that such uses are permitted under applicable state and federal laws;

B. Disclose PHI in its possession for proper management and administration purposes or to fulfill any present or future legal responsibilities of Business Associate, provided that Business Associate represents to Covered Entity, in writing, that (i) such disclosures are required by law, or (ii) Business Associate has received reasonable assurances from the party to whom the information is disclosed that it will be held confidentially and consistent with the requirements of 45 C.F.R. § 164.504(e)(4)(ii)(B)(l); and

C. Aggregate the PHI in its possession with the PHI of other covered entities that Business Associate has in its possession through its capacity as a Business Associate to other covered entities; provided, the purpose of such data aggregation is to provide Covered Entity with data analyses relating to the Health Care Operations of Covered Entity.

5. Responsibilities of Covered Entity.

With regard to the use and/or disclosure of PHI by Business Associate, Covered Entity agrees:

A To provide Business Associate with a current copy of its Notice of Privacy Practices ("Notice");

B. To notifY Business Associate, in writing and in a timely manner, of any arrangements that may impact the use and/or disclosure of PHI by the Business Associate under the terms of this Addendum; and

C. Not to request that the Business Associate use or disclose PHI in any manner that would not be permitted under HIPAA if done by the Covered Entity, except for Data Aggregation or management and administrative activities of the Business Associate.

6. Term and Termination.

A *Term.* This Addendum shall become effective on the Effective Date and shall continue in effect until all obligations of the Parties have been met, unless previously terminated as provided in this Section 6.

B. *Termination.* Covered Entity may immediately terminate this Addendum and any related agreements, including the Agreement, if Covered Entity reasonably determines that Business Associate has breached a material term of this Addendum. Alternatively, Covered Entity may: (i) provide Business Associate with 30 days written notice of the existence of an alleged material breach; and (ii) afford Business Associate an opportunity to cure the alleged material breach upon mutually agreeable terms. Nonetheless, in the event that mutually agreeable terms cannot be achieved within 30 days, such a failure to cure the alleged material breach shall be grounds for the immediate termination of this Addendum.

C. *Automatic Termination.* This Addendum will automatically terminate without any further action of the Parties upon the termination or expiration of the Agreement.

7. MISCELLANEOUS.

A. *Survival.* The respective rights and obligations of Business Associate and Covered Entity under the provisions of Sections 3, 4 and 5 solely with respect to PHI Business Associate retains in accordance with Section 3(K) because it is not feasible to return or destroy such PHI, shall survive termination of this Addendum indefinitely.

B. *Amendments; Waiver.* This Addendum may not be modified, nor shall any provision hereof be waived or amended, except in a writing duly signed by authorized representatives of the Parties. A waiver with respect to one event shall not be

construed as continuing, or as a bar to or waiver of any right or remedy as to subsequent events. The parties agree to enter into a mutually acceptable amendment to this Addendum as necessary to comply with then-current, applicable federal and state laws and regulations governing the use and/or disclosure of individually identifiable health information (including without limitation HIPAA and the Privacy Rule), all of which may be subject to future change.

C. *No Third Party Beneficiaries.* Nothing express or implied in this Addendum is intended to confer, nor shall anything herein confer, upon any person other than a Party any rights, remedies, obligations, or liabilities whatsoever.

D. *Notices.* Any notices to be given hereunder to a Party shall be governed by the Agreement.

E. *Counterparts and Facsimile.* The Parties may execute this Addendum in counterpart hereto. The Parties may exchange signatures to this Addendum by facsimile and such signatures shall be deemed to be original and effective to bind the Parties

F. *Integration.* This Addendum shall be incorporated into and made part of the Agreement. This Addendum and the Agreement constitute the entire agreement of the Parties regarding the subject matter set forth herein and therein and supersede all prior oral and written agreements regarding such subject matter. In the event that any term or provision of this Addendum contradicts or conflicts with a term or provision of the Agreement, that term or provision of this Addendum shall control.

G. *Regulatory References.* A reference in this Addendum to a section in the Privacy Rule and/or the Security Rule means the section as in effect or as amended, and for which Covered Entity's compliance is required.

H. *Interpretation.* Any ambiguity in this Addendum shall be resolved in favor of a meaning that permits compliance with the Privacy Rule and/or the Security Rule, as applicable.

IN WITNESS WHEREOF, each of the undersigned has caused this Business Associate Addendum to be duly executed in its name and on its behalf effective as of the Effective Date.

_____
(Covered Entity)

By: _____ By: _____

_____, Executive Director

Print Name: _____

Print Title: _____ Date: _____

Date: _____

-

User Responsibility Statement and Agreement for use of BRCAN-HMIS Systems (example)

Agency Name: _____ Date: _____

User's Name: _____ User's Position/Title: _____

User's Work Email: _____ User's Work Number: _____

User Responsibility Statement

Please initial each item below to indicate your understanding of proper access to BRCAN-HMIS Systems. Any failure to uphold the standards set forth below is grounds for immediate termination of your user name/system access and notification of the Agency Director.

By placing my initials next to each of the statements below, I affirm that I understand the following:

My user name and password are for my use only and may not be shared with others. I will take all reasonable means to keep my password private and physically secure.

The only individuals who can view BRCAN-HMIS Systems information are authorized users and the individual client to whom the information pertains.

I may only view, obtain, disclose or use BRCAN-HMIS Systems information necessary to perform my job.

I will observe the client authorization and verification policy and process detailed in any BRCAN-HMIS User Training Manual / Guide.

I will enter accurate, complete information to the best of my ability.

Hard-copy printouts of BRCAN-HMIS Systems individual client data are part of a client's confidential file and must be kept in a secure location. If they are no longer needed they must be properly destroyed to maintain confidentiality.

A computer running BRCAN-HMIS Systems should never be left unattended. If I am logged into any BRCAN-HMIS System, I must log off before leaving my work area.

I understand that these rules apply to all users of BRCAN-HMIS Systems, whatever their role or position.

If I notice or suspect a security or confidentiality breach, I will immediately notify BRCAN-HMIS staff.

In order to receive my account information promptly, I agree to pass the Confidentiality Training class with a score of 70% or higher as soon as the course is available within my region. I agree to pass this course within 90 days or my account information will be revoked.

I agree to maintain strict confidentiality of information obtained through BRCAN-HMIS Systems. Any breach of confidentiality will result in notification of the agency director and immediate termination of my participation in BRCAN-HMIS Systems.

User Signature _____ Date: _____

Agency Director Signature _____ Date: _____

BRCAN-HMIS Community Network Client Authorization Form

I understand that Council of Community Services (CCS) (this agency) is part of the BRCAN-HMIS Community Network, a computer network designed to reduce the amount of time and effort it takes for me to obtain the social services I need. This agency has my permission to:

- Look at information about me in the BRCAN-HMIS system
- **Enter in the system information concerning my situation and need for assistance**

I understand that:

- Agencies in the BRCAN-HMIS system will keep this information confidential
- Other agencies will be able to look at this information only if I give each of these **Agencies my permission**
- Staff at each Agency receives regular training on client confidentiality and their legal responsibility to keep my information private
- The BRCAN-HMIS system uses passwords and computerized codes to protect my privacy
- Shared information may include my name, age, gender, marital status, veteran status, address, housing status, and basic information about my goals and the services I receive
- I can obtain a copy of information about me collected by the BRCAN-HMIS system, except for psychotherapy notes and other information kept private by law.

I also understand that I have the right to refuse to grant this authorization, and that even if I give permission for this agency to access my information in the BRCAN-HMIS system, I can revoke that permission at any time, without penalty. The permission I am giving this agency to view my information and to place information about me in the BRCAN-HMIS system will expire on:

_____

I also understand that under certain circumstances, this agency or BRCAN-HMIS may be legally required to disclose some or all of my confidential information. This may happen if there is any evidence of child abuse, if there is evidence I may harm others or myself, or if a court orders that my information be disclosed.

In order to improve services for persons in need, experts may study data from the BRCAN-HMIS system and other sources. As a result, an independent researcher may need to view personal information, such as names and Social Security numbers, to make sure that records are not counted twice. This researcher will remove all personally identifiable information before anyone else examines the data, so that the privacy of those who received services is protected. This procedure is done in accordance with professional standards, under strict government and research institution supervision, and in compliance with all regulations that specifically address those who have received services for mental health, substance abuse, HIV/AIDS, and domestic **violence.**

I authorize this agency to view my information, and to place information about me in the BRCAN-HMIS system.

Signature:_____ Date:_____

Print Name:_____ ID:_____ Date of Birth:_____

Witness Signature:_____

Rev. 7-5-2005

Attachment 5

"REFERRAL ONLY" AGENCY

Request Form example

REFERRAL ONLY Agency Profile Information

(This section refers to the Agency you would like included in BRCAN)

Referral Agency Name : (The name the agency does business as)	
Referral Agency's Legal Name : (If different from the Agency Name)	
Address:	
City, State, Zip:	
Main phone:	Fax:
Agency Contact Name:	Agency Contact Email:
"Hide" the Agency's Address?: DYes ONo	
Agency Website (Optional):	
Has this agency agreed to be listed as a "Referral Agency" that accepts *referrals* from other agencies? DYes D No	
If so, has the Agency Contact above agreed to receive referral notifications by email? DYes D No	
Does this agency provide housing of any kind (emergency, transitional, permanent, etc.)? DYes D No	
If so, please select one housing type (please check one box only): ☐ Men's ☐ Women's ☐ Children's ☐ Family ☐ Coed	

Services this Agency Provides

Service Code	Description

REQUESTING Agency Information

(This section refers to the Agency making the request)

Agency Name:	
Your Name:	
Your Title:	
Your phone number:	
Your Email Address:	
Your Signature:	Date:

Attachment 6

Blue Ridge Continuum of Care
Grievance Report/Appeal Form

We ask that you include at least your name so that we can prove that this is a legitimate grievance and attempt to resolve it.

Contact Information: _____ _____
First Last

Street Address City/State Zip

Your Phone Number/Other Contact: _____

Your Email (if you have one) _____

Agency you are complaining about: _____

Have you followed the agency's grievance procedure? _____Yes _____No

Specific Grievance/Incident date, Persons Involved/Grievance Explanation: (include any witnesses)

_____

_____

_____

_____

_____

_____

_____

- o I do not want this information made public.
- o I do not mind if this information is made public.
- o I do not mind if this information is made public, but I do not want my name used.

I certify that the information is true, and that information about this grievance.

_____ _____
Client Signature Date Submitted

_____ _____
Received By Date

Attachment 7

SAMPLE site data collection notice, to be posted in accordance with Policy 2-1:

Blue Ridge Community Assistance Network (Blue Ridge CAN) Data Collection & Sharing

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 needed and appropriate.
We protect your Privacy and Confidentiality every way we can, using industry standard methods to do so.

We will ONLY Share this data with Your Permission, and ONLY with Our Community Partners who have AUTHORIZED and SECURE access to the Blue Ridge CAN. Your data is NEVER shared outside the Blue Ridge CAN without your knowledge and permission, such as for Research in ways to help you.
We do need your permission to Share, in order to provide the best assistance we can to you.

BRCAN-HMIS COMMUNITY NETWORK

Family Consent Form

I understand that **Council of Community Services (CCS)** (the "Agency") is part of the BRCAN-HMIS COMMUNITY NETWORK, a computer network that consists of certain organizations that participate in connection with the provision of human services and/or related administrative activities ("Participating Organizations"). The purpose of the BRCAN-HMIS COMMUNITY NETWORK is to reduce the amount of time and effort it takes to process and administer requests for human services to which I/we may be entitled. Through the BRCAN-HMIS COMMUNITY NETWORK, Participating Organizations have access to information maintained under the internet-based system known as the BRCAN-HMIS COMPASS SYSTEM.

Personal Information:

For purposes of this form, "Personal Information" shall mean any and all personal and individually identifYing information regarding myself, and any minors for whom I am legally responsible, that is provided or obtained in connection with human services requested or received by myself and any such minors. Personal Information may include (but will not necessarily be limited to) name, age, gender, marital status, veteran status, address, housing status, social security number, and basic information about the goals and the services requested/received by myself and any such minors.

The Agency has my consent ("Consent") to:

- Access and use all Personal Information collected in the BRCAN-HMIS COMPASS SYSTEM in connection with the processing of any request by me for human services, the provision of any such services on behalf of myself or any minor for whom I am legally responsible, and/or any related administrative activities;

- Enter Personal Information into the BRCAN-HMIS COMPASS SYSTEM;

- Disclose Personal Information to Participating Organizations in connection with the processing of any request by me for human services, the provision of any such services on behalf of myself or any minor for whom I am legally responsible, and/or any related administrative activities; and

- Disclose Personal Information to independent researchers under the following circumstances:

  In order to improve services for persons in need, experts may need to study data maintained in the BRCAN-HMIS COMPASS SYSTEM. As a result, an independent researcher may need to view various items of Personal Information such as names and social security numbers to ensure that records are not counted twice or to otherwise ensure the validity and integrity of the study being conducted. I hereby consent to Agency granting any such researcher(s) access to Personal Information with the understanding that such person(s) will be required to remove all personally identifiable information before anyone else can examine the data and that this procedure will be done in accordance with applicable professional standards, under strict government and research- institution supervision, and in compliance with all regulations that specifically address services for mental health, substance abuse, HID/AIDS, and domestic violence.

Initials

PATHWAYS COMPASS

BRCAN-HMIS COMMUNITY NETWORK

Family Consent Form

In granting such Consent, I understand that:

- My Consent to the access, use, and disclosure of Personal Information by Agency extends to and includes such access, use, and disclosure by Participating Organizations;
- Agency and Participating Organizations will use and have access to such Personal Information in connection with my request/receipt of human services, system maintenance and improvement, and related administrative activities but will otherwise strive to keep this information confidential;
- Any agencies other than Agency and Participating Organizations will be permitted access to such Personal Information only ifI give each such agency my written permission;
- Staff at Agency and each Participating Organization are required to receive regular training on client confidentiality and responsibilities in maintaining the confidentiality of information such as Personal Information;
- The BRCAN-HMIS COMPASS SYSTEM uses passwords and computerized codes designed to protect my privacy and that of any minors for whom I am legally responsible; and
- I can obtain a copy of Personal Information maintained in and accessible via the BRCAN-HMIS COMPASS SYSTEM, except for psychotherapy notes and other information to the extent required to be kept private by law.

I also understand that:

- I have the right to refuse to grant this Consent, and such refusal will not affect my eligibility, if any, or that of any minor for whom I am legally responsible, with respect to any human services;
- Even ifI grant this Consent, I can revoke it in writing at any time without penalty; The permission I am giving this agency to view my information and to place information about me in the BRCAN-HMIS COMMUNITY NETWORK will expire on:

  10/30/2016

- Under certain circumstances, Agency or a Participating Organization may be legally required to disclose some or all of the Personal Information covered under this Consent outside of the BRCAN-HMIS COMMUNITY NETWORK. Examples of where this may occur include (i) where there is any evidence of child abuse, (ii) where there is evidence I may harm others or myself, or (iii) where a court orders that any such Personal Information be disclosed. The Consent that I am granting by signing below extends to and includes any and all such disclosures.

_____
Initials

PATHWAYS COMPASS

BRCAN-HMIS COMMUNITY NETWORK

Family Consent Form

And, in granting this Consent, I acknowledge that:

I am signing this form freely and have not been forced or coerced to do so. This consent form has been read by me or to me, and ▮ have received a copy of this form. ▮ have been given the opportunity to discuss the content of this form and the Consent being granted under it, and ▮ have been given the opportunity to ask any questions regarding such content and Consent. Any such questions have been answered to my full satisfaction, and I understand the Consent that I am granting by signing below.

By: _____ _____
(My signature) Date

Print Name: _____

To ensure there is no fraudulent use of this consent form, a head of household must be specified, and the names and dates of birth for any and all minor children for whom I am legally responsible must be listed below.

Head of Household (please print):

_____ _____
Name DOB

Minors' Names and Dates of Birth (please print):

_____ _____
NAME DOB

_____ _____
NAME DOB

_____ _____
NAME DOB

_____ _____
NAME DOB

_____ _____
NAME DOB

BRCAN-HMIS Notice of Privacy Practices Certification

"Council of Community Services (CCS) is part of the Blue Ridge Community Assistance Network (BRCAN-HMIS), a computer network designed to reduce the amount of time and effort it takes for consumers to obtain the human services they need. This agency has policies and procedures to protect confidential information people give us when we talk to them on the phone. This agency's Notice of Privacy Practices is available to you. It describes:

- the types of information that we consider confidential
- the ways we protect this information
- permitted uses and disclosures of this information, and
- your rights concerning this information

You can pick up a copy of our Notice of Privacy Practices at our offices during normal business hours, or you can download the Notice from our web site. I will also be glad to read the Notice to you now."

I have read the above notice in its entirety to the person named below, have given the person the opportunity to have the agency's Notice of Privacy Practices read in its entirety, and to ask questions about our privacy practices. I have answered all questions to the best of my ability and training.

Certified By: _____ Date: _____

Printed Name: _____

Agency Use Only:

Client name: _____ Date of Birth: _____

SSN: _____ Mother's Maiden Name: _____

Other Identifying Information: _____

BRCAN-HMIS Notice of Privacy Practices Certification

Certification Procedure

It is the intention of all BRCAN-HMIS stakeholder agencies to provide services to all eligible clients regardless of their location when initiating contact with our agencies. The *vast* majority of BRCAN-HMIS client Authorizations are made in person at a participating human services agency. In some cases, however, the client is not able to travel to an agency for a conventional client intake. This may be due to a lack of transportation, geographic distance, or handicap. In these cases, staff at participating agencies may use the Notice of Privacy Practices, utilizing the following procedure:

1. Obtain at least three types of identifying information (i.e.: name, date of birth, social security number, mother's maiden name).

2. Read the BRCAN-HMIS Notice of Privacy Practices Form to the client.

3. Ask if the client has any questions about what she/he has heard. Answer any questions.

4. If the client agrees, print the client's identifying information (from list above) in the Agency Use Only area of the form. Place your initials next to the information.

5. Sign and date the Certification form in the "Certified By" and "Date" spaces and print your name below your signature.

If you have any questions about this procedure, please contact:
the BRCAN-HMIS Support Team.

Attachment 10

BRCAN-HMIS Client Opt-Out Form

I understand that a member of my household recently received services from Council of Community Services (CCS) (the Agency) and provided basic information about me that was entered into the BRCAN-HMIS Community Network collaborative case management system. This basic information may have included:

-My name
- My date of birth
- My gender, race, and ethnicity
- Income that I contribute to my household.

I understand that:
- Agencies that use the BRCAN-HMIS will keep this information confidential
- Other agencies will be able to look at this information only if I give each of these agencies my permission
- Staff at each agency that uses the BRCAN-HMIS receives regular training on client confidentiality and their legal responsibility to keep my information private
- The BRCAN-HMIS uses passwords and computerized codes to protect my privacy
- Depending on the Agency's rules, I can either view or obtain a copy of information about me collected by the BRCAN-HMIS system, except for psychotherapy notes or other information kept private by law.

I also understand that I have the right to "opt-out" and prevent the Agency from further use of my information, and even if I don't opt-out now, I can do so at any time, without penalty.

I also understand that under certain circumstances, the Agency or BRCAN-HMIS may be legally required to disclose some or all of my confidential information. This may happen if there is any evidence of child abuse, if there is evidence I may harm others or myself, or if a court orders that my information be disclosed.

To opt-out, sign and date this form and return it to Council of Community Services (CCS).
There is no need to sign or return this form if you do not wish to opt-out at this time.

I do not want the Agency to have access to my information.

Signature:,_____ Date:_____

Name: _____

Agency Contact:_____Telephone:_____

Agency Name: Council of Community Services (CCS)

Attachment 11

User Policy for Blue Ridge Community Assistance Network (Blue Ridge CAN)

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[1]."

The Blue Ridge Community Assistance Network (Blue Ridge CAN) 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 Blue Ridge CAN 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.

Blue Ridge CAN 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 Blue Ridge CAN 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 Blue Ridge CAN Client Release of Information form.
All Blue Ridge CAN Users are required to attend Blue Ridge CAN training sessions prior to using the system.
All Blue Ridge CAN Users are required to complete a privacy training specific to protecting information contained within Blue Ridge CAN prior to using the System.
All Blue Ridge CAN Users are required to have read and understand their Agency's Privacy Notice.