Homeless Management Information System (HMIS) Policies and Procedures

Blue Ridge Interagency Council
On Homelessness (BRICH) Approved:
October 13, 2023

Table of Contents

I. Introduction

Overview

The Homeless Management Information System (HMIS) is a web-based database that is used by homeless service providers within the Blue Ridge Continuum of Care (BRCoC) to record and store client-level information to coordinate care and better understand the characteristics and needs of persons experiencing homelessness and those at-risk of homelessness. Additionally, HMIS enables programs to measure the effectiveness of their interventions, share information between service providers for case coordination, and facilitate longitudinal analysis of service needs and gaps. Current HMIS Vendor and Software information are contained within the Appendix of HMIS Policy and Procedures. The Council of Community Services (CCS) is the HMIS Lead Agency and Administrator, managing the system, including, but not limited to, managing user licensing, training, data analytics, technical assistance, and compliance. Specific information about governance about HMIS operations can be found in the Blue Ridge Interagency Council on Homelessness (BRICH) Governance Charter. Guidance for the implementation of HMIS is provided by BRICH and its subcommittees including the HMIS Steering and Coordinated Entry System Advisory Committees.

This document provides the policy guidelines and standards that govern HMIS operations, as executed by the HMIS Lead Agency and also describes the responsibilities of Participating Agencies and users. It was approved by the BRICH on _____ and replaces all earlier documents.

Federal HMIS Policies

In addition to the BRCoC HMIS Policies contained herein, our HMIS must also comply with federal HMIS requirements. These requirements are detailed in a suite of HMIS Data Standard resources, an overview of which is provided below:

Manual Name	Intended Audience	Contents
HMIS Data Standards Dictionary	HMIS Vendors & HMIS Lead Agencies	The manual provides the detailed information required for system programming on all HMIS elements and responses required to be included in HMIS software. It delineates data collection requirements, system logic, and contains the XML and CSV tables and numbers. The manual also includes critical information about data collection stages, federal partner data collection required elements, and metadata data elements.

HMIS Data Standards Manual	HMIS Lead Agencies & HMIS Users	The manual provides a review of all of the Universal Data Elements and Program Descriptor Data Elements. It contains information on data collection requirements, instructions for data collection, and descriptions that the HMIS User will find as a reference.

Both manuals can be found at the following web address:
https://www.hudexchange.info/resource/3824/hmis-data-dictionary/

HMIS documents should be typically reviewed and updated each year, and changes tend to be effective October 1st, in line with the Federal Fiscal Year. The Steering Committee will review HUD standards when they are released, update any policies in this manual, and present the changes to BRICH. HMIS Federal Partner Program Manuals contain additional detailed information on HMIS project setup and data collection for federally-funded programs:

- Continuum of Care Program (CoC) Manual
- Emergency Solutions Grant (ESG) Program Manual
- Housing Opportunities for Persons with AIDS (HOPWA) Program Manual
- Projects for Assistance in Transition from Homelessness (PATH) Program Manual
- Runaway and Homeless Youth (RHY) Program Manual
- Veteran Affairs (VA) Program Manual
- VA Data Guide
- Youth Homelessness Demonstration Program (YHDP) Manual

Participation in HMIS

A. Required Participation

Projects who are funded by some HUD funding and Virginia Department of Housing and Community Development (DHCD) funding are required to enter information into HMIS. Examples of HUD or DHCD projects that require HMIS participation include but are not limited to:

- Community Development Block Grant (CDBG)
- Emergency Solutions Grant (ESG)
- Housing Opportunities for Persons Living with AIDS (HOPWA)
- HUD Continuum of Care (COC)
- Projects for Assistance in Transition from Homelessness (PATH)
- Runaway and Homeless Youth (RHY)
- Supportive Services for Veteran Families (SSVF)

- Virginia Homeless Solutions Program (VHSP)
- Virginia Housing Trust Fund (HTF)

The list above is not exhaustive and other funding sources may require participation in HMIS. All agencies that provide services and housing to the homeless are encouraged to participate in HMIS. Please note: while Agencies execute the HMIS Partnership Agreement, User Access is granted based on Project participation level.

Victim Service Providers (VSP's) are required to collect and enter data in a comparable database. The HMIS lead is responsible for ensuring that the comparable database meets all HUD specifications related to privacy, security, data standards and reporting. Victim Service Provider agencies must collaborate and adhere to the state's HMIS procedure for data collection within their own comparable database. Programs are required to collect client level data consistent with HMIS data collection requirements. To protect clients, VSPs must enter all required client level data into a comparable database that complies with HMIS reporting requirements.

B. Voluntary Participation

The BRCoC strongly encourages any homeless service providers to fully participate with all of their homeless projects, regardless of their funding source. Agencies/projects who do not receive funding that requires HMIS participation may participate in HMIS as a Non-HUD agency.

Voluntary Participation in HMIS can include:

- Non-HUD: A Non-HUD agency is an agency that has an operating project they want to collect data for in HMIS (SO, ES, TH, PH, SSO) but is not required by a HUD, State or local funding source to collect within HMIS;
- Informational Agency - an agency that does not have any operating projects in HMIS (SO, ES, TH, PH, SSO). There is no data entered under the informational agency. The agency is documented as a "Participating Agency'' within our HMIS for the purpose of Client Consent. Agencies shall be eligible to become an Informational Agency if they meet the following criteria:
  - Agency is a direct provider of services or programming to persons experiencing homelessness;
  - Agency is NOT a direct provider of services or programming to persons experiencing homelessness but does work with persons experiencing homelessness (e.g. medical care) and desires to participate in HMIS for the sole purpose of assisting their clients to be enrolled in the CoC's Coordinated Entry System (CES)

- Future Coordinated Entry Participation – If the Steering Committee determines that expansion of our CES Access Points is desired, we could create additional agency participation categories.

Voluntary Participants must adhere to all requirements for documentation, monitoring and training that are set forth for a Required Agency. Examples of these requirements include but are not limited to: Participating Agency Agreement, End User License Agreements for all end users, training and monitoring.

While the BRCoC cannot require non-funded providers to participate in the HMIS, the BRCoC works closely with all agencies working with persons experiencing homelessness to articulate the benefits of the HMIS and to strongly encourage their participation. HMIS data provides the best overview available of homelessness in our CoC, and this information is used to redirect services, funding, and resources as needed.

Points of Contact

HMIS users should submit all questions, requests for technical assistance, troubleshooting or reports to the BRCoC HMIS Help Desk. HMIS staff is available for Technical Assistance, questions, and trouble-shooting Monday to Friday, 8:30am-4:30pm.

HMIS Steering Committee

The HMIS Steering Committee focuses on strategic policy issues facing the HMIS as well as submits reports and policy decisions to the BRICH for review and adoption by the BRCoC. The Committee will focus on issues such as data sharing, data quality, data standards, privacy, security, and confidentiality plans, and the role of HMIS in coordination of services, performance metrics, and report generation. The Committee generally meets monthly, no less than once per quarter, with the Steering Committee Chair coordinating the agenda, sending out meeting notices, and recording/sharing the minutes. Policy updates will be presented to the committee prior to submission to the BRICH. Updates approved by the HMIS Steering Committee shall be presented to the BRCoC at the next regularly scheduled meeting.

The HMIS Steering Committee membership shall consist of a chair nominated and voted upon by the membership of the committee, the HMIS Lead, the CoC Lead, the HMIS Administrator and other staff, and at least 4 other members who represent subject matter experts for the various service providers (ie. Shelter, SO, PATH, Veterans, etc.). The HMIS Lead shall not serve as the chair of the Steering Committee but can fill in when there is no appointed chair or may chair meetings when the chair is not available and no other designee has been assigned.

The HMIS Steering Committee will work with the HMIS Lead on the following (but not limited to):

- Develop, annually review, and, as necessary, revise for Board approval a privacy plan, security plan, and data quality plan for the HMIS and all other policies and procedures required by regulations and notices issued by the Department of Housing and Urban Development;

- Develop for BRICH approval and implement a plan for monitoring the HMIS to ensure that:
    - HMIS is satisfying the requirements of all regulations and notices issued by the Department of Housing and Urban Development; and
    - The HMIS Lead is fulfilling the obligations outlined in its memorandum of agreement with the BRCOC, including the obligation to enter into written participation agreements with each contributing HMIS organization.

The HMIS Steering Committee Executive Committee will consist of the Steering Committee Chair, HMIS Lead, CoC Lead, and one at-large member. The at-large member shall be an end user of HMIS who is a Subject Matter Experts (SME's) who possess strong working knowledge in Data Privacy and Security, Data Matching, Data Reporting and Analysis and/or Database Administration.

- Resignation and Removal: Any member may resign from the committee at any time with notice given to the Chair. In addition, members may be removed from their positions by a majority vote of remaining members. Removal of members should be limited to issues of negligence with the HMIS system or lack of participation.
- Recusal: Members of the committee may not vote on issues that involve a clear conflict of interest.

Roles and Responsibilities of the Executive Steering Committee: All members need to be in good standing in order to serve on the Executive Committee. The chair or their designee will preside over meetings of the HMIS Steering Committee and the Executive Committee.

Duties of the Executive Committee Members at large:

- Establishing Ad Hoc working groups;
- Evaluating the conduct of directors, especially their compliance with the conflict of interest and attendance policies, as set forth in this manual;
- Evaluate the overall operations of the HMIS
- Meaningful participation and ongoing attendance
- Participate in designating a HMIS software vendor

- Oversee and approve the development and implementation of HMIS Policies and Procedures, a Data Quality Plan, and a Security and Privacy Plan
- Ensure compliance to those documents through monitoring.

Amending the Policies and Procedures

These Policies and Procedures may be amended. It is expected that information shall be added, removed, and altered as necessary. If a change is deemed necessary, it will be vetted by the HMIS Steering Committee and presented to the BRICH for adoption by the BRCoC. Any changes suggested by any party in the BRCoC shall be presented by a member of the HMIS Steering Committee or any HMIS staff member to the HMIS Steering Committee. This policy may be amended at any time and the amendments may impact information obtained by the Participating Agency before the date of the change. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.

II. On-Boarding of New Agencies to HMIS

On-Boarding Procedures

Agencies who seek access to HMIS must submit a new agency request form and/or a letter to the HMIS Steering Committee detailing the following:

1. Agency Information
   a. Contact Information;
   b. Organizational Mission and Work Undertaken;
   c. Documentation that the organization is a government agency or non-profit (with an IRS determination letter, Board of Directors approval, and approved Bylaws);
   d. Documentation the organization has been in operation for over one year;
   e. Agency Privacy and Data Controls; and,
   f. Current Release of Information (if applicable)
2. Reason for Access Request
   a. Intent & Plan for Usage;
   b. Justification for Direct Access to HMIS, as opposed to coordinating with Project Provider/Coordinated Entry Staff;
3. Description of the Staff who will use HMIS; and,
4. Any Other Relevant Information

The Request will be reviewed and approved via vote at the next Monthly HMIS Steering Committee meeting. The HMIS Lead will send any urgent requests for access to the Executive Committee of the HMIS Steering Committee. Urgent requests will take at least 3 business days

to process. This section does not apply to the HMIS Lead agency (and its consultants/ contractors), the HMIS Steering Committee Chair, the person(s) conducting the work to complete the CoC Collaborative Application, and other users designated by the HMIS Steering Committee. The HMIS Steering Committee may also approve access to other entities for the purposes of research, analysis, and reporting as described in this document.

The procedure for onboarding new agencies into HMIS is as follows:

1. BRCoC HMIS team to Contact the Agency to discuss joining HMIS and its requirements (ie., annual Security Audits, Workstation requirements; all detailed in new user onboarding).
2. Agency steps to complete:
    a. Identify an HMIS Agency Captain - see section below.
    b. Complete HMIS Partnership Agreement with signatures from the Executive Director of the Participating Agency (or their designee) and HMIS Lead Staff (or their designee) from the Council of Community Services.
    c. Complete the New Agency set-up form online located here to provide the HMIS Team with information about your organization.
    d. Complete the project set-up form located here to set up project(s) in HMIS according to funding source and client population.
    e. Schedule a new user HMIS training with the HMIS System Administrators that consists of the following areas:
        I. HMIS system overview – adding clients, enrolling in projects, adding services, case notes, etc.
        II. HMIS security & privacy overview – client consent, workstation safety, passwords, client PII & PPI, document storage and disposal.
        III. Workstation Desk Audit - All new users will need to complete a workstation desk audit to confirm security and privacy standards are met before having access to HMIS
3. Training is considered complete when all overview training and the workstation audit has been completed by System Administrators. (In the future, if the CoC has implemented a Learning Management System (LMS), the overview trainings may be completed by the users independently. Training would be complete after System Administrators have reviewed the knowledge check results in the LMS and completed the workstation audit).

Overview of Participating Agency Requirements

1. Collecting Data for HMIS

   Agencies and projects participating in the HMIS should collect personal client information for all clients served. If client consent is not obtained, the client enrollment for this agency record will be locked by the end user. All information entered under the locked enrollment will only be visible to the agency entering the information. Client information gathered with consent allows personal information to be shared with other Partnering Agencies within HMIS, when appropriate, for the provision of services and/or for other specific purposes of the organization and/or when required by law. Clients cannot be denied services for choosing not to share data in HMIS.

   Purposes for which agencies/projects collect protected personal information (PPI) may include the following:

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

2. Eligible HMIS Users

   Participating Agencies/projects must have at least one staff member or volunteer who is eligible to become an HMIS user. Users must be paid staff or official volunteers of an Agency. An official volunteer must complete a volunteer application with the Participating Agency, undergo agency training, and record volunteer hours within their participating agency.

   Individuals who are solely contracting with a Participating Agency must be subject to the same vetting and training as staff and volunteers who become HMIS users. All users must be at least 18 years old and possess basic computer skills. The Participating Agency is responsible for the actions of its users and for their training and supervision, in accordance with the Agency Agreement. The HMIS team is not responsible for basic computer training outside of HMIS data input.

3. Adding New Users to HMIS

Once an organization is approved as a Participating Agency, new users can be requested by completing the New User form. Without a completed new user request form, the HMIS team will not proceed in adding any trainees.

4. Assigning Access Roles

Our HMIS allows for staff to be assigned different levels of access that align with the end-user's roles and responsibilities within their agency/project. The new user request form must be fully completed, including details of the end-user's position/title, their purpose in HMIS, etc,. The new user request will not be processed until all this information is provided to the HMIS team.

5. Different access Roles

The access roles available in HMIS include, but are not limited to:

a. Agency Staff - primarily for end-users who are required to enter or cleanup data under their Home Agency
b. Reports Only - primarily for end-users who are responsible for monitoring or their work requires data from other agencies
c. HMIS Agency Captain – Main HMIS contact at each agency. Single source for requesting new user accounts. Oversees training & compliance.
d. Standalone attendance – Scan stations for meals or other services.
e. Referral Matchmaker – CES position that refers client from Community Queue to a housing program
f. Agency Referral Manager - primarily for end-users that are responsible to accept/deny referrals for their agency's shelter/housing projects
g. CES - Staff Member - primarily for end-users that are entering/updating data under Coordinated Entry

Participating Agency Captain Requirements

Agencies must designate one key staff person to serve as Agency Captain. This person is responsible for the oversight of all personnel that generate or have access to client data in the HMIS to ensure adherence to the Policies & Procedures described in this document, as well as federal policies and procedures, including HUD publications and updates in the Federal Register. Typically, the Agency Captain responsibilities include:

1. Administering the requests for access and monitoring agency staff access and use of the HMIS;
2. Ensuring compliance with all HMIS policies and procedures through oversight and training of staff, and through creating agency policies that support HMIS policies;

3. Preventing staff misuse of the data system by means of training and policy;
4. Restricting access to the HMIS to staff who have received proper training, and who have a legitimate need for access (need exists only for those staff who work directly with clients, who supervise staff who work directly with clients, research or have data entry or technical responsibilities);
5. Following procedure changes as determined by the HMIS Steering Committee or state and federal regulation;
6. Implementing and maintaining data security policies and standards, in compliance with the HMIS Data Privacy Policies (see below) and any other applicable policies;
7. Administering agency-specified data protection controls;
8. Aiding in and/or coordinating the recovery of data, when necessary;
9. Detecting and responding to violations of federal, HMIS or agency Policies and Procedures;
10. Accepting and processing any HMIS-related grievances submitted by clients;
11. Generating Data Quality reports readily available in the database for Agency projects, and/or reviewing such reports or custom data quality reports generated by HMIS Staff, in order to address data gaps and inconsistencies, at regular intervals each grant year.
12. Notify the HMIS Systems Administrator of changes within the Agency Profile, bed counts, projects, and when HMIS users leave their agency through the appropriate online forms or the helpdesk.

HMIS General Service Agreement

Agencies must sign and abide by the HMIS Partnership Agreement, a document agreement made between the participating agency and the Council of Community Services (HMIS Lead). This agreement includes a commitment to enter information on clients served within the agency's participating projects. This document is the legally binding document that refers to all laws and/ or regulations relating to privacy protections and information sharing of client specific information. Without an executed agreement, the BRCoC HMIS team will not proceed in adding any projects or end-users in the HMIS.

Security

Agencies must ensure compliance with requirements set forth by Federal and State law along with additional security protocols set forth in this document including securing and transmission of Protected Personal Information (PPI; including through unencrypted email). Refer to the following guidance available on our website:

1. BRCoC HMIS Required Workstation Security Policy & Compliance Checklist
2. BRCoC HMIS Password Policy
3. BRCoC HMIS Personal Protected Information Privacy Policy
4. BRCoC HMIS Data Collection Statement

Training

Agencies will ensure that all users meet the mandatory training and onboarding programming requirements. Users who are not trained and/or don't have a current HMIS license in their name, shall not under any circumstances be allowed access to HMIS.

New Users must:

Successfully complete onboarding training that includes the following:

1. Watching the videos relevant to their position in the Clarity HMIS Basics YouTube playlist (https://www.youtube.com/channel/UCgAjAZDwQUucVWZy1WRf-sw)
2. Live training with an HMIS System Administrator that includes an HMIS system overview and HMIS security & privacy overview.
3. A workstation desk audit conducted by their Agency HMIS Captain.

Group refresher trainings and Data Quality support are offered by the HMIS System Admins on a monthly basis in the BRCoC Data Quality meetings and on demand. Training is provided at no cost to users.

At the discretion of the HMIS Lead, HMIS Agency Captain, or BRCoC, it may be determined that a user needs to be re-trained and/or that access to HMIS shall be limited until sufficient training can be provided to the user to ensure successful participation in HMIS as to not affect system data quality.

HMIS End-User Agreement

All new end users are required to electronically sign the “End User Agreement” through HMIS as soon as they successfully login for the first time. By signing the agreement, the End User confirms that they understand and will comply with the full scope of HMIS privacy policies, policies regarding access to HMIS, and this document. The HMIS System Administrators may update the End User Agreement as necessary to reflect new policies or HUD requirements. All HMIS users will be required to sign the agreement once per year.

Data Quality

In accordance with the HUD Data and Technical Standards, End Users and Agency HMIS Captains will familiarize themselves with the HMIS Data Quality and Monitoring Plan, enter data according to HMIS and HUD Standards and cooperate fully with Program Managers and HMIS Staff in correcting aberrations from these standards. The HMIS Lead will hold monthly Data Quality review meetings to provide DQ review and technical assistance for all Participating

Agencies. The HMIS will send out DQ reports with instructions for reviewing DQ to all Agency HMIS Captains prior to the monthly meetings. DQ meetings will also be a time for update or refresh training for staff.

Maintenance of On-Site Computer Equipment

Executive Director or designee of each participating agency/project will be responsible for the maintenance and disposal of on-site computer equipment and data used for participation in the HMIS including the following:

1. Computer Equipment: The Participating Agency/project is responsible for maintenance of on-site computer equipment. This includes purchase of and upgrades to all existing and new computer equipment for utilization of HMIS.
2. Internet Connection and Web-Browsers: The Participating Agency/project is responsible for maintaining internet connections compatible with daily HMIS usage and troubleshooting problems. Clarity HMIS requires the latest release of one of the following web browsers: Microsoft Edge, Mozilla Firefox, Google Chrome, or Apple Safari.
3. Data Storage: The Participating Agency/project agrees to only download and store data in an encrypted format, using industry standard access controls to secure the data. This may include the use of encrypted archive files such as secured WinZip/PKZip, or the use of operating system security such as data encryption in conjunction with the implementation of system policies to enforce individual user profiles and user authentication. PPI data may not be uploaded/ stored on public sites.
4. Data Disposal: The Participating Agency/project 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.

III. Operational Procedures

User Accounts

User accounts will be created and archived by the HMIS Systems Administrators. The HMIS System Administrator team generates a unique user code for each new End User. Participating Agencies required to request new users on HMIS through the online process referenced above. Agency HMIS Captains are required to notify the HMIS Lead within 24 hours of an end user's separation of employment to ensure that the user's access is deactivated and to report on when end-users are no longer in need of HMIS within 24-hours after their termination/need of access.

Designation of User Access Levels

There are different levels of access to the HMIS. These permissions are granted based on data entry and management needs. The System Administrator team will grant users the access level with the fewest permissions possible that will allow the user to accomplish their job effectively. See the User Role Table or equivalent in Appendix for details.

Passwords

Password resets are a function of the software, and should be initiated by the end user for access to the system. End users may reset their own password on HMIS directly. It is the responsibility of the End Users to reset their passwords as needed and to create passwords that meet password security guidelines set forth in the HMIS Password Policy and Federal HMIS regulations. For more information on password security, please see the BRCoC HMIS User Agreement and Password Policy.

Restricting Access

Permission to use the HMIS and the data stored on HMIS is based on the agreement to protect all sensitive data. Usernames and Passwords are only provided to qualified End Users with legitimate need for access, and inactive user accounts are promptly disabled by the Systems Administrator team. No HMIS license is to be shared and will result in an immediate revocation of HMIS access. Further, information obtained from use of the HMIS cannot be shared with any entity that also does not have permission to use information stored on the HMIS System. Finally, information obtained from the HMIS System may only be used strictly within all federal, state, and local laws and within all guidelines set by the HMIS Steering Committee.

Auditing Access

The Systems Administrator team can audit HMIS for unauthorized or questionable access of data as a routine security check, or at the request of Agency HMIS Captains or Program Managers.

Using HMIS Data for Research

The HMIS Steering Committee will review and respond to requests for the use of HMIS data for research. Approval or denial will be voted on by the committee with the majority having the final decision. In the event of an urgent request, the HMIS Lead will send any urgent requests for research to the Executive Committee of the BRCoC HMIS Steering Committee. Urgent requests will take at least 3 business days to process.

The following procedures will be followed:

- No client PPI will be released without a proper data use agreement (DUA) (see below for research criteria utilizing Personally Identifying Information (PII);
- Requested data will be available in the form of an aggregate report
- De-identified raw data set requests must be approved by the HMIS Steering Committee
- Documentation, including the parameters of the data set will be presented with each report;
- Research results will be reported to the HMIS Steering Committee prior to publication, for publication approval by the HMIS Steering Committee;
- Research will be shared with the appropriate agencies after publication; and,
- HMIS Steering Committee will be granted the rights to utilize all findings (results).

Research can be carried out by:

1. An individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a program administrator (other than the individual conducting the research) designated by the Participating Agency. OR
2. An institution for use in a research project conducted under a written research agreement approved in writing by a program administrator designated by the Participating Agency.

A written research agreement must:

1. Establish rules and limitations for the processing and security of PPI in the course of the research.
2. Provide for the return or proper disposal of all PPI at the conclusion of the research.
3. Restrict additional use or disclosure of PPI, except where required by law.

4. Require that the recipient of data formally agree to comply with all terms and conditions of the agreement.

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

Disaster Recovery Plan

Disaster recovery for the BRCoC HMIS will be led by the HMIS Vendor with support from HMIS Participating Agencies. The HMIS System Administrator must be familiar with the disaster recovery plan set in place by the HMIS software vendor. A copy of the disaster recovery plan will be posted on the BRCoC HMIS webpage at www.endhomelessnessblueridge.org/hmis.

IV. Technical Support

Service requests may be initiated by participating HMIS agency staff to address concerns including, but not limited to, problems logging into HMIS, accessibility within the system, duplicate clients, clarification on data standards, changing bed inventories, adding or removing users, adding or removing projects, problems with data sharing and pulling reports.

The procedure for a Participating Agency to initiate a technical service request is as follows:

1. End user informs Agency Captain of the problem.
2. Agency Captain attempts to resolve the issue. If unable to resolve, agency staff may contact HMIS staff via helpdesk using the online form: HMIS Help Desk.
3. HMIS staff investigates and addresses the problem or concern if possible.
4. HMIS staff determines resources needed for service and if necessary, contacts vendor for support.
5. Service requests and responses may occur through email, telephone, or in-person appointment as needed.
6. Service requests are handled as promptly as possible, often immediately, but service requests will be prioritized at the discretion of the HMIS System Administrators based on their current workloads and the urgency of the request.

V. Requests for Software Feature Changes and/or Feedback

Users and stakeholders with requests for software feature changes and/or feedback shall address their concerns to the HMIS Team and/or the HMIS Steering Committee. Requests for new data elements or questions shall be directed to the HMIS Lead and are not considered Software feature changes.

VI. Data Sharing

Data Ownership:

The CoC Program Interim Rule gives CoCs authority over and responsibility of HMIS. Data ownership questions are addressed through the HMIS Steering Committee and the CoC Governing Board (BRICH). Ultimately, clients own their personal data. When seeking services, client must consent any data collection and sharing policies. Additional information on who owns the data in HMIS can be found on the HUD Exchange's HMIS FAQ's Page.

Client Release of Information

BRCoC Data Sharing is a process guided by the client through the Release of Information. It is therefore imperative that the client understand the ROI, and that the Participating Agency/project address any questions the client may have, while respecting the client's right to decline to share data.

Prior to entering information into HMIS, the Participating Agency/project shall attempt to obtain the informed (written or verbal) consent of the Client, with written consent preferred, using the HMIS Release of Information. If a client does not consent, pursuant to the HMIS Release of Information (ROI) form, the information will still be entered into HMIS and the record will be locked by the HMIS System Administrators to ensure that client data is not be shared within HMIS.

It is the responsibility of the agency/project entering information about a client to determine whether consent has been obtained; to make appropriate entries to either designate the information as appropriate for sharing or prohibit information sharing; and to implement any restrictions on information sharing.

At a minimum, the Participating Agency/project must meet the following standards:

1. The Participating Agency/project will use the HMIS Release of Information form (ROI), for all clients where written or verbal consent is required. If questions arise (for example questions on which programs within the Participating Agency/project share data with other agencies), the Participating Agency/project should consult the agency list on the HMIS webpage. If there are still unanswered questions about data sharing, the PA/project will contact the Lead Agency.
2. The Participating Agency/project will note any limitations or restrictions on information sharing on a client's ROI with appropriate data entries into HMIS. If questions arise (for example, questions on how to implement restrictions on information sharing), the Participating Agency/project will contact the HMIS Lead.

3. The Participating Agency/project will be responsible for ensuring that consent is understood and given by a person competent to provide consent. For example, in the case of a minor, the Participating Agency/project will comply with applicable laws regarding minor consent and obtain the consent of a parent or guardian.
4. If a client withdraws or revokes consent for release of information, the Participating Agency/project is responsible for immediately locking down the enrollment to their Agency to ensure that client's information will not be shared with other Agencies/projects from that date forward.
5. The Participating Agency/project is responsible for making sure the ROI is reflected in HMIS by creating an ROI entry in the client's profile. An electronic signature or uploaded pdf document can be attached to the ROI entry if desired. Verbal consent is sufficient for initial Coordinated Entry engagement; however, it is advisable to obtain written consents as soon as possible. Agencies/projects who collect HIPPA data or engage in Medicaid billing are advised to adhere to all relevant regulations. Participating Agencies/projects may be required to keep the original copy for a period of seven years, as required by the Participating Agency policy or funder requirements. ROI forms will be available for inspection and copying by the Lead Agency at any time.
6. If an ROI has been properly recorded in the client's HMIS record by another Participating Agency, the Participating Agency/project still needs to present the client with another ROI form giving permission for your agency to enter client data into the HMIS. HIPAA Covered Entities must always present a ROI form, as detailed in the section below.

Additional Responsibilities of Covered Entities (HIPAA)

Participating Agencies that are also Covered Entities under the Health Insurance Portability and Accountability Act (HIPAA) and any program subject to 42 CFR Part 2 must obtain a signed HMIS Release of Information form before authorizing the Participating Agency or HMIS Lead Agency to use or disclose information entered into the HMIS. The Participating Agency/project agrees to indemnify and hold the HMIS Leading Agency harmless against any claims that data or information was entered, stored or otherwise used in violation of HIPAA or any other privacy law by that Participating Agency/project.

The information may be used by the Lead Agency as permitted by law and the HMIS Data Privacy Notice. It is the responsibility of the Participating Agency entering information about a client to ensure compliance with HIPAA including ensuring that all appropriate HIPAA Notices have been provided to clients, to determine whether consent has been obtained; making appropriate entries to either designate the information as appropriate for use or disclosure by the Lead Agency or to prohibit such use or disclosure; and implementing any restrictions on the use of the information.

The requirement to scan and upload signed Consent forms is effective as of the date these policies were first adopted. Client records created prior to that date that recorded Consent according to the guidance from that time are considered to have Consent properly recorded. Participating Agencies may utilize their own forms but shall supplement these forms with the information conveyed in this document. Participating Agencies must present a separate ROI form to each adult that is seeking services, regardless of whether a ROI form has been presented to them in the past.

No Conditioning of Services based on Release of Information

Participating Agencies/projects will not condition any services upon or decline to provide any services to a client based upon a client's refusal to sign a form for the sharing of information in HMIS. In cases where a program funder or internal management practice requires the entry of identified information into the HMIS to deliver services, client data must be restricted from sharing if no consent is obtained. Further, Participating Agencies may not limit client service or refuse to provide service in a way that discriminates against clients based on information the Participating Agency/project obtained from the HMIS. Participating Agencies may not penalize a client based on historical data contained in the HMIS.

Sharing of Attachments

Uploaded client documents and attachments can be shared throughout the BRCoC, depending where the agency staff saves the documents within HMIS and provided the client has signed a consent to have that information shared as of the date indicated on the signed release. Sharing of attachments will allow for better care coordination, support coordinated entry, reduce duplication of collection of vital documents, and ensure safe digital keeping of important client record.

Reporting Access

Generally, individual Participating Agencies shall only have access to pull reports on their own specific programs, activities, and projects. Organizations may enter into agreements with one another to allow other organizations access to agency/project reports and aggregate data.

HMIS Participating Agencies may also submit a request to the HMIS Steering Committee to have the HMIS System Administrators pull a report that includes other participating agencies (e.g. organization wants a report on all rapid rehousing outcomes, not just their own programs). Any requests submitted to the HMIS Steering Committee will be shared with the organizations whose data is requested and their input sought, before a final decision is made.

VII. Privacy

1. Introduction

The HMIS Lead Agency, Participating Agencies, and End Users are jointly responsible for complying with HMIS privacy policies and procedures. When a privacy standard conflicts with other federal, state and local laws to which the Participating Agency must adhere, the Participating Agency must contact the Lead Agency to collaboratively update the applicable policies for the Participating Agency to accurately reflect the additional protections. Each agency agrees to indemnify and hold harmless the HMIS Lead Agency against any allegations that it entered, stored or otherwise used information in a manner that did not meet the requirements of the Baseline Privacy Statement. We intend our Privacy Plan to support our mission of providing an effective and usable case management tool. We recognize that clients served by individual agencies are not exclusively that "agency's client" but instead are truly a client of the BRCoC. Thus, we have adopted a Privacy Plan which supports an open system of client-level data sharing amongst agencies.

2. Goal

The goal of the HMIS Privacy Policy is to ensure that all required client data will be captured in the HMIS while maintaining the confidentiality and security of the data in conformity with all current regulations related to the client's rights for privacy and data confidentiality. It is recognized that Participating Agencies may have established their own privacy policies that meet the HUD privacy requirements and minimum standards set forth below. One purpose of this document is to outline those standards and define the parameters of compliance with these standards. The document is not intended to supplement individual privacy policies. As long as Participating Agencies' policies and practices meet the minimum thresholds established in this policy and do not interfere with the practices described in this policy, Participating Agencies and projects may establish additional or more stringent requirements.

HMIS Privacy and Security standards are set forth by HUD and outlined in HUD's standards for Homeless Management Information Systems, which can be found here: https://www.hudexchange.info/programs/hmis/hmis-data-and-technical-standards/

Additionally, HUD provides for specific requirements in the updated, published Coordinated Entry Management Guide: https://www.hudexchange.info/resource/5758/coordinated-entry-management-and-data-guide/

3. Baseline Privacy

The core tenant of our Privacy Plan is the Baseline Privacy Statement. The Baseline Privacy Statement describes how client information may be used and disclosed and how clients can get access to their information.

Each agency must either adopt the Baseline Privacy Statement or develop a Privacy Statement which meets and exceeds all minimum requirements set forth in the Baseline Privacy Statement (this is described in the Agency Responsibilities section of this Privacy Plan). This ensures that all agencies who participate in the HMIS are governed by the same minimum standards of client privacy protection.

Summary Required Elements & Documents	
Baseline Privacy Statement: This is the main document of this Privacy Plan. This document outlines the minimum standard by which an agency collects, utilizes, and discloses information.	Agencies/projects must adopt a privacy statement which meets all minimum standards. It is must be posted on your Agency's local website (if available).
Consumer Notice Posting: This posting explains the reason for asking for personal information and notifies the client of the Privacy Notice.	Agencies/projects must adopt and utilize a Consumer Notice Posting.
Consumers Informed Consent, Sharing & Release of Information Authorization: This form must be signed by all adult clients and unaccompanied youth. This gives the client the opportunity to refuse sharing of their information to other agencies within HMIS.	Written or verbal consent of the Client, with written consent preferred are required prior to inputting their information in HMIS in a manner that is shared. Agencies/projects must "lock" or restrict access to others once a client revokes consent or denies sharing.

4. End User Privacy Responsibilities

A client's privacy is upheld only to the extent that the users and direct service providers protect and maintain client privacy. The role and responsibilities of the user cannot be over-emphasized. A user is defined as a person that has direct interaction with a client or their data. (This could potentially be any person at the agency: staff member, volunteer, contractor, etc.) Each End User agrees to indemnify and hold harmless the HMIS Lead Agency against any allegations that it did not comply in any manner with the End User Privacy Responsibilities.

Users have the responsibility to:

a. Understand their agency's Privacy Statement
b. Be able to explain their agency's Privacy Statement to clients
c. Follow their agency's Privacy Statement
d. Know where to refer the client if they cannot answer the client's questions
e. Must complete Consumers Informed Consent, Sharing & Release of Information Authorization with client prior collecting HMIS data.
f. Present their agency's Privacy Statement to the client before collecting any information
g. Uphold the client's privacy in the HMIS

5. Participating Agency Responsibilities

Agencies have the responsibility to:

- Review their program requirements to determine what industry privacy standards must be met that exceed the minimum standards outlined in this Privacy Plan and Baseline Privacy Statement (examples: Substance Abuse Providers covered by State Law, 24 CFR Part 2, HIPPA Covered Agencies, Legal Service Providers).
- This Privacy Plan and the Baseline Privacy Statement provide guidance on the minimum standards by which agencies/projects must operate if they wish to participate in the HMIS. Meeting the minimum standards in this Privacy Plan and the Baseline Privacy Statement are required for participation in the HMIS. Any agency may exceed the minimum standards described and are encouraged to do so. Agencies/projects must have an adopted Privacy Statement which meets the minimum standards before data entry into the HMIS can occur. w the 2004 HUD HMIS Privacy Standards (69 Federal Register 45888)
- Adopt and uphold a Privacy Statement which meets or exceeds all minimum standards in the Baseline Privacy Statement as well as all industry privacy standards. The adoption process is to be directed by the individual agency. Modifications to the Baseline Privacy Statement must be presented to the HMIS Steering Committee and approved by the BRCoC.
- Ensure that all clients are aware of the adopted Privacy Statement and have access to it. If the agency/project has a website, the agency/project must publish the Privacy Statement on their website.
- Make reasonable accommodations for persons with disabilities, language barriers, or education barriers.
- Ensure that anyone working with clients covered by the Privacy Statement can meet the User Responsibilities.
- Designate at least one Security Officer (may be Agency Captain) that has been trained to uphold technologically the agencies adopted Privacy Statement.

Each HMIS Participating Agency must have a Privacy Statement that describes how and when the Participating Agency/project may use and disclose clients' Protected Personal Information (PPI). PPI includes but is not limited to name, Social Security Number (SSN), date of birth, project entry and/or exit date, and unique personal identification number (HMIS Unique Identifier).

Participating Agencies/projects may be required to collect some PPI by law, or by organizations that give the agency money to operate their projects. PPI is also collected by Participating Agencies/projects to monitor project operations, to better understand the needs of people experiencing homelessness, and to improve services for people experiencing homelessness. Participating Agencies/projects are only permitted to share PPI with a client's written/verbal consent.

6. Use and Disclosure of Information

   Participating Agencies may use and disclose client PPI to:

   - Provide or coordinate services to clients;
   - Locate other programs that may be able to assist clients;
   - For functions related to payment or reimbursement from others for services that are provided;
   - Operate the agency, including administrative functions such as legal, audits, personnel, oversight, and management functions;
   - Comply with government reporting obligations;
   - When required by law; and for research purposes.

Participating Agencies are obligated to limit disclosures of PPI to the minimum necessary to accomplish the purpose of the disclosure. Uses and disclosures of PPI not described above may only be made with a client’s written consent. Clients have the right to revoke consent at any time by submitting a request in writing.

7. Clients Access to Records

   Clients also have the right to request from HMIS:

   - A copy of all PPI collected;
   - An amendment to any PPI used to make decisions about your care and services (this request may be denied at the discretion of the agency, but the client’s request should be noted in the project records);
   - An account of all disclosures of client PPI;
   - Restrictions on the type of information disclosed to outside partners; and,
   - A current copy of the Participating Agency’s privacy statement.

Participating Agencies may reserve the right to refuse a client's request for inspection or copying of PPI in the following circumstances:

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

If a client's request is denied, the client should receive a written explanation of the reason for the denial. The client has the right to appeal the denial by following the established Participating Agency/project grievance procedure. Regardless of the outcome of the appeal, the client shall have the right to add to his/her program records a concise statement of disagreement. The Participating Agency/project shall disclose the statement of disagreement whenever it discloses the disputed PPI.

8. Privacy Training

All new users are required to complete the privacy training in order to gain access to the HMIS. All individuals with access to PPI are required to complete formal training in privacy requirements at least annually.

9. Participating Agency Privacy Statements

Participating Agency Statements should, at a minimum, reflect the baseline requirements listed in this document and the HMIS Data and Technical Standards Final Notice, published by HUD in July 2004, and revised in March 2010. In any instance where this Privacy Statement is not consistent with the HUD Standards, the HUD Standards take precedence except where an agency is acting as a HIPAA entity Participating Agency Privacy Statements may be amended at any time. Amendments may affect information obtained by the agency before the date of the change. An amendment to the Privacy Statement regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. A record of all amendments to this Privacy Statement must be made available to clients upon request.

VIII. **Security**

1. Security Plan Overview

HMIS security standards are established to ensure the confidentiality, integrity, and availability of all HMIS information. The security standards are designed to protect against any reasonably anticipated threats or hazards to security and must be enforced by system administrators, agency managers, as well as end users. This section is written to comply with section 4.3 of the 2004 Homeless Management Information Systems (HMIS) Data and Technical Standards Final Notice (69 Federal Register 45888) as well as local legislation pertaining to maintaining an individual's personal information. The last time HUD has released proposed regulations pertaining to HMIS Security was in December of 2013. These regulations are not yet in force and sufficient guidance has not been given to enact the policies.

The HMIS and all agencies/projects must apply the security standards addressed in this Security Plan to all the systems where PPI is stored or accessed. Additionally, all security standards must be applied to all networked devices. This includes, but is not limited to, networks, desktops, laptops, mobile devices, mainframes, and servers. All agencies/projects, including the HMIS Lead, will be monitored by the HMIS Administrators annually to ensure compliance with the Security Plan. Agencies/projects that do not adhere to the security plan will be given a reasonable amount of time to address any concerns. Egregious violations of the security plan may result in immediate termination of an agency or user's access to the HMIS as determined by the HMIS Lead.

2. Security Officers

The HMIS Lead Agency and all HMIS Participating Agencies must designate Security Officers to oversee HMIS privacy and security. The security officer, who can be the Agency Captain, is the single point-of-contact who is responsible for annually certifying that Agencies adhere to the Security Plan testing the CoC's security practices for compliance.

Systemwide Security Officer

Position held by the HMIS Lead and is responsible for:

- Assessing security measures in place prior to establishing access to HMIS for a new Agency,
- Reviewing and maintaining file of Participating Agency/project annual compliance certification checklists,
- Conducting annual security audit of all Participating Agencies/projects.

Participating Agency/Project Security Officer

Position fulfilled within a Participating Agency, may be the Agency Captain or another employee, volunteer or contractor who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance.

This person:

- Conducts a security audit for any and all workstations that will be used for HMIS purposes,
- Continually ensures each workstation within the Participating Agency/project used for HMIS data collection or entry is adequately protected by a firewall and antivirus and malware software (per Technical Safeguards - workstation computer policy),
- Completes the annual Compliance Certification Checklist and forwards the Checklist to the Systemwide Security Officer.

Upon request, the HMIS Lead Agency may be available to provide security support to Participating Agencies who do not have the staff capacity or resources to fulfill the duties assigned to the Participating Agency Security Officer.

3. Physical Safeguards

In order to protect client privacy, it is important that the following physical safeguards be put in place. For the purpose of this section, authorized persons will be considered only those individuals who have completed Privacy and Security training within the past 12 months.

a. Computer Location - A computer used as an HMIS workstation must be in a secure location where only authorized persons have access. The workstation must not be accessible to clients, the public or other unauthorized Participating Agency/project staff members or volunteers.

b. A password protected automatic screen saver will be enabled on any computer used for HMIS data entry.

c. Printer location - Documents printed from HMIS must be sent to a printer in a secure location where only authorized persons have access.

d. PC Access (visual) – Non-authorized persons should not be able to see an HMIS workstation screen. Monitors should be turned away from the public or other unauthorized Participating Agency/project staff members or volunteers and utilize visibility filters to protect client privacy.

e. Mobile Device – A mobile device used to access and enter information into the HMIS system must use a password or other user authentication on the lock screen to prevent an unauthorized user from accessing it and it should be set to lock automatically after a set period of device inactivity. A remote wipe and/or remote disable option should also be downloaded onto the device.

4. Technical Safeguards

Workstation Security

Participating Agency Security Officer will confirm that any workstation accessing HMIS shall have antivirus, anti-malware software with current virus definitions (updated at minimum every 24 hours) and frequent full system scans (at minimum weekly).

Participating Agency Security Officer will confirm that any workstation accessing HMIS has and uses a hardware or software firewall either on the workstation itself if it accesses the internet through a modem or on the central server if the workstation(s) accesses the internet through the server.

5. Rescinding User Access

The Participating Agency must notify the HMIS System Administrator within 24 hours if an End User no longer requires access to perform his or her assigned duties due to a change of job duties or termination of employment. The HMIS Administrator reserves the right to terminate End User licenses that are inactive for 60 days or more. The HMIS Administrator will attempt to contact the Participating Agency to confirm that the End User in question no longer needs HMIS access prior to termination of the user's license.

In the event of suspected or demonstrated noncompliance by an End User with the HMIS End User Agreement or any other HMIS policies, forms, standards or governance documents, the Participating Agency/project Security Officer shall notify the HMIS Administrator to deactivate the End User in question until an internal agency investigation has been completed. The HMIS Lead Agency should be notified of any substantiated incidents that may have resulted in a breach of HMIS security and/or client confidentiality, whether or not a breach is definitively known to have occurred.

Any agency personnel who are found to have misappropriated client data (identity theft, releasing personal client data to any unauthorized party), shall have HMIS privileges revoked. The BRCoC is empowered to revoke permanently a Participating Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the BRCoC HMIS Policies and Procedures, or the HMIS Privacy Statement that resulted in a release of PPI.

6. Workstation Security

HMIS Users will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

Specific measures include:

a. Restricting physical access to workstations to only authorized personnel;
b. Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access;
c. Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected;
d. Complying with all applicable password policies and procedures;
e. Ensuring workstations are used for authorized business purposes only;
f. Never installing unauthorized software on workstations;
g. Storing all sensitive information, including protected health information (PHI) on network servers;
h. Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets;
i. Ensuring workstations are updated regularly or left on but logged off in order to facilitate IT after-hours updates. Remember To exit running applications and close open documents;
j. Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup); and,
k. If wireless network access is used, ensure access is secure by following the Wireless Access policy

Workstations include any areas or devices used to access HMIS or undertake work on HMIS (including spaces at home, office, and remote locations). Specific devices include but are not limited to laptops, tablets, phones, mobile devices, desktops, and computer based medical equipment.

7. Disposing Electronic, Hardcopies, Etc.

Computer: All technology equipment (including computers, printers, copiers and fax machines) used to access HMIS and which will no longer be used to access HMIS will have their hard drives reformatted multiple times (DoD specifications). If the device is now non-functional, it must have the hard drive pulled, destroyed, and disposed of in a secure fashion.

Hardcopies: For paper records, shredding, burning, pulping, or pulverizing the records so that PPI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.

Mobile Devices: Use software tools that will thoroughly delete/wipe all information on the device and return it to the original factory state before discarding or reusing the device.

8. Other Technical Safeguards

The Lead Security Officer shall develop and implement procedures for managing new, retired, and compromised HMIS account credentials.

The Participating Agency Security Officer shall develop and implement procedures for managing new, retired, and compromised local system account credentials. The Participating Agency Security Officer shall develop and implement procedures that will prevent unauthorized users from connecting to private agency networks.

Unencrypted PPI may not be stored or transmitted in any fashion-including sending file attachments by email or downloading reports including PPI to a flash drive, to the End User's desktop or to an agency shared drive. All downloaded files containing PPI must be deleted from workstation temporary files and the "Recycling Bin" emptied before the End User leaves the workstation.

9. Reporting Security Incidents

A security incident is defined as but not limited to the following:

- Unauthorized Access to HMIS (including after separation or position change)
- Client information gathered/shared without client consent
- Failure to adhere to security and privacy policies, including workstation security and password security
- Unauthorized release of client Personally Identifying Information (PII)
- Use of HMIS data for research without proper approval

All security incidents may be reported to either the HMIS Lead Agency or the HMIS Steering Committee. The Agency Captain and the HMIS Lead Agency are responsible for investigating all substantiated and reported incidents (including hearsay or third-party reports).

These standards are intended to prevent, to the greatest degree possible, any security incidents. However, should a security incident occur, the following procedures should be followed in reporting address the concern:

1. When it is suspected that HMIS system security and/or client privacy has been compromised the Agency Captain must notify HMIS via helpdesk ticket to immediately suspend access. If the HMIS lead is aware, they will immediately suspend access to the end user or agency. In the event that HMIS suspends access, the HMIS team will notify the Agency Captain immediately via email that includes the nature of the security concern (if applicable).

2. The HMIS Lead must immediately report the concern to the Executive members of the BRCoC HMIS Steering Committee via emergency meeting or email.
3. Internal Investigation: Immediately upon suspension, an internal investigation shall be completed by the Lead Security Officer.
    a. The Investigation shall be completed within 5 full business days following the suspension.
    b. The investigation shall include
        i. An interview with the Agency Captain of the Agency
        ii. An interview with the end user(s) whose license is suspended
        iii. HMIS consultation with their privacy and security legal counsel
        iv. Any key informants identified by the end user, Lead Security Officer or Agency Manager
    c. In the event that an investigation cannot be completed within the 5 full business days, the HMIS team shall request an extension from the Executive Members of the HMIS Steering Committee in writing including:
        i. The original dates the investigation was scheduled to occur
        ii. Factors leading to the request for extension
        iii. Extension request date
        iv. The extension request shall be CC'd to the Agency Manager involved
    d. Upon conclusion of the investigation, the Lead Security Officer shall provide the Executive Members of the RIHMIS Steering Committee with a Memo detailing:
        i. The reason for the suspension action
        ii. Key pieces of information gathered during the investigation
        iii. The final determination of the HMIS Lead Security Officer
            1. <u>If the access is reinstated</u>: Indicate that access will be reinstated and any terms of reinstatement (retraining, increased auditing, etc)
            2. <u>If the access is not reinstated and the end user's access is permanently disabled</u>: Indicate specific elements of the BRCoC HMIS Policies & Procedures or End user agreement that were violated (using as much supporting evidence as possible)
        iv. The Lead Security Officer may require the Agency Captain to establish a written action plan to mitigate any future security concerns (see section e).
        v. In the event of a security breach related to client PPI, the Lead Security Officer will notify the Agency Captain if there needs to be a disclosure (see section f).
        vi. The right to appeal the decision in writing to the Chair of the HMIS Steering Committee within 7 days of receipt of the Memo
    e. Action Plan:

i. The action plan shall be implemented as soon as possible, and the total term of the plan must not exceed thirty (30) days.
ii. If the Participating Agency/project is not able to meet the terms of the action plan within the time allotted, the HMIS Agency Captain, in consultation with the BRICH, may elect to terminate the Participating Agency's/project's access to HMIS. The Participating Agency/project may appeal to the BRICH for reinstatement to HMIS following completion of the requirements of the action plan.

f. Client PPI Disclosure:
i. In the event of a substantiated release of PPI in noncompliance with the provisions of these Security Standards, the BRCoC HMIS Policies and Procedures, or the Participating Agency/project Privacy Statement, the Participating Agency/project Security Officer will make a reasonable attempt to notify all impacted individual(s).
ii. The Lead Security Officer must approve of the method of notification and the Participating Agency/project Security Officer must provide the Lead Security Officer with evidence of the Agency's notification attempt(s). If the Lead Security Officer is not satisfied with the Agency's/project's efforts to notify impacted individuals, the Lead Security Officer will attempt to notify impacted individuals at the Agency's expense.

g. At the conclusion of an investigation, the HMIS Lead Agency will notify the BRICH via Memo within 30 days of any substantiated release of PPI in noncompliance with the provisions of these Security Standards, the HMIS Policies and Procedures, or the Participating Agency Privacy Statement.

h. The HMIS Lead Agency will maintain a record of all substantiated releases of PPI in noncompliance with the provisions of these Security Standards, the BRCoC HMIS Policies and Procedures, or the Participating Agency Privacy Statement for 7 years.

i. The Continuum of Care reserves the right to revoke permanently a Participating Agency's users' access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the BRCoC HMIS Policies and Procedures, or the Participating Agency Privacy Statement that resulted in a release of PII.

10. New HMIS Participating Agency Site Security Assessment

Prior to establishing access to HMIS for a new Participating Agency, the Lead Security Officer will assess the security measures in place at the Participating Agency to protect client data (see Technical Safeguards Workstation Security). The Lead Security Officer or other HMIS Lead will meet with the Participating Agency Executive Director (or executive level designee) and Participating Agency Security Officer to review the

Participating Agency's information security protocols prior to countersigning the HMIS Memorandum of Understanding. This security review shall in no way reduce the Participating Agency's responsibility for information security, which is the full and complete responsibility of the Participating Agency, its Executive Director, and its HMIS Agency Security Officer.

11. Annual Participating Agency Self-Audits

- The Participating Agency Security Officer will use the HMIS Security Compliance Checklist to conduct annually security audits of all Participating Agency HMIS End User workstations.
- The Participating Agency Security Officer will audit for inappropriate remote access by End-Users by associating User login date/times with employee time sheets. End Users must certify that they will not remotely access HMIS from a workstation (i.e.: personal computer) that is not subject to the Participating Agency Security Officer's regular audits.
- If areas are identified that require action due to noncompliance with these standards or any element of the BRCoC HMIS Policies and Procedures, the Participating Agency Security Officer will note these on the Checklist, and the Participating Agency Security Officer and/or HMIS Agency Manager will work to resolve the action item(s) within 30 days.
- Any Checklist that includes 1 or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved. The findings, action items, and resolution summary must be reviewed and signed by the Agency's Executive Director or other empowered officer prior to being forwarded to the Lead Security Officer.
- The Participating Agency Security Officer must turn in a copy of the Checklist to the Lead Security Officer on an annual basis.

12. Bi-Annual Security Audits

- The Lead Security Officer will use the Annual HMIS Security Compliance Checklist to conduct security audits every two years of all Participating Agencies.
- The Lead Security Officer will audit at least 30% of the workstations used for HMIS data entry that also represent a good cross-section of user access roles (agency staff, agency captain, reports-only, etc.) and workstation locations (ie. shared, single-user, mobile devices, etc.) In the event that an agency has more than 1 project site, at least 1 workstation per project site must be audited.
- If areas are identified that require action due to noncompliance with these standards or any element of the BRCoC HMIS Policies and Procedures, the Lead Security Officer will

note these on the Checklist, and the Participating Agency/project Security Officer and/or HMIS Agency Captain will work to resolve the action item(s) within 30 days.

- Any Checklist that includes 1 or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved and the findings, action items, and resolution summary has been reviewed and signed by the Agency's/project's Executive Director or other empowered officer and forwarded to the HMIS Lead Security Officer.

IX. Client Complaints, Grievances, and Questions

If a client believes that their rights have been violated related to their personal or private data held in the HMIS, a written complaint may be filed. The complaint may be filed with the Participating Agency serving the client and forwarded to the HMIS Lead Agency if resolution is not found. If the client believes that their shelter or services may be threatened due to the complaint, a complaint may be made directly to the HMIS Lead Agency. The Lead Agency will report all grievances to the HMIS Steering Committee (which reports to the BRICH).

The HMIS Steering Committee will act as a final arbiter of any complaints not resolved by the Participating Agency or the Lead Agency.

The Participating Agency and HMIS Lead Agency are prohibited from retaliating against clients for filing a complaint. Identifying information will be kept confidential, unless the client gives express permission for such information to be shared between the Participating Agency and the HMIS Lead Agency.

X. Violation of HMIS Policies

HMIS users and Participating Agencies must abide by all HMIS policies and procedures found in the HMIS Policies and/or Procedures manuals, the User Agreement, and the Agency Agreement.

Participating Agency or user access may be suspended or revoked for suspected or actual violation of these policies, particularly the security protocols. Serious or repeated violation by users of the system may result in the suspension or revocation of a participating agency's access.

The procedure to be followed is:

1. All suspected violations of any security protocols will be investigated by the Participating Agency and the HMIS Lead.
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 HMIS privileges, and revocation of HMIS privileges.

3. Access may be restricted prior to completion of formal investigation if deemed necessary by the HMIS Lead. If access is restricted, the HMIS Lead will notify a chair of the HMIS Steering Committee of the restriction and will consult with them about next steps.
4. Any Participating 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 HMIS Steering Committee.

Notifying the HMIS Lead Agency of a Violation

It is the responsibility of each Participating Agency HMIS Captain and user(s) to notify the HMIS Lead Agency within 24 hours of when they suspect that a User or Participating Agency has violated any HMIS operational agreement, policy, or procedure. A complaint about a potential violation must include the User and Participating Agency name and a description of the violation, including the date or time frame of the suspected violation. Complaints should be sent in writing to the HMIS Lead Agency. The name of the person making the complaint will not be released from the HMIS Lead Agency if the individual wishes to remain anonymous.

Violations of Local, State or Federal Law

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

Suspension or Termination of HMIS Access

During an investigation, an active HMIS end-user will have their access suspended or terminated until the results of the investigation from the BRHMIS Steering Committee's Executive Committee are determined.

XI. Glossary and Definitions

AHAR - Stands for the Annual Homeless Assessment Report; HUD (the United States Department of Housing and Urban Development) uses the AHAR to report to U.S. Congress that provides nationwide estimates of homelessness. Utilizes data from the LSA (definition below).

CAPER – Stands for the Consolidated Annual Performance and Evaluation Report; Generated to report on accomplishments and progress towards consolidated plan goals.

CoC APR – the HUD Continuum of Care (CoC) Annual Performance Report (APR) is used for any recipients with HUD funding received through CoC homeless assistance grants are required to submit an APR electronically to HUD every operating year.

Continuum of Care (CoC) - A Continuum of Care (CoC) is a regional or local planning body that coordinates housing and services funding for homeless families and individuals.

Continuum of Care (CoC) Governing Board – the Blue Ridge Interagency Council on Homelessness (BRICH) serves as the CoC Board.

HEARTH Act- On May 20, 2009, President Obama signed the Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH) Act of 2009. The HEARTH Act amends and reauthorizes the McKinney-Vento Homeless Assistance Act with substantial changes; including a consolidation of HUD's competitive grant programs, the creation of a Rural Housing Stability Assistance Program, a change in HUD's definition of homelessness and chronic homelessness, a simplified match requirement, an increase in prevention resources and emphasis on performance.

HITECH means the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-005 - created to stimulate the adoption of electronic health records (EHR) and the supporting technology in the United States.

HIC – Stands for Housing Inventory Count; HUD requires CoC's to conduct an annual count of homeless persons and the HIC is a point-in-time inventory pf provider programs within a CoC that provide beds and units dedicated to serve persons who are homeless, categorized by five program types: Emergency Shelter (ES), Transitional Housing (TH), Rapid Re-Housing (RRH), Safe Haven (SH), and Permanent Supportive Housing (PSH).

HMIS - Stands for Homeless Management Information System, which is a local information technology system used to collect client-level data and data on the provision of housing and services to homeless individuals, families, and persons at risk of homelessness.

HMIS Lead Agency - The HMIS Lead Agency is the Council of Community Services. This entity is designated by the Continuum of Care to operate the Continuum's HMIS on its behalf.

HMIS Steering Committee - Comprised of HMIS stakeholders, this committee focuses on strategic and policy issues facing the HMIS, such as data sharing, data quality standards, performance metrics, privacy, security, and report generation.

HUD - The United States Department of Housing and Urban Development is a Cabinet department in the Executive branch of the United States federal government that funds

permanent housing and emergency shelter services for homeless and formerly homeless individuals and families. An HMIS system is required by HUD for all CoCs receiving HUD funding.

Longitudinal Systems Analysis (LSA) report - used to inform the AHAR, is produced from a CoC's Homelessness Management Information System (HMIS) and submitted annually to HUD via the HDX 2.0, provides HUD and Continuums of Care (CoCs) with critical information about how people experiencing homelessness use their system of care.

Participating Agency - An Agency within the CoC that creates, edits or views HMIS data.

PIT – Stands for Point-in-Time count; HUD requires a count of sheltered and unsheltered homeless persons on a single night in January - this count includes persons who are sheltered in an Emergency Shelter (ES) or Transitional Housing (TH) as well as those unsheltered on the street or in a place not meant for human habitation. PITs are collected annually including the last Wednesday of each quarter.

Project - A distinct unit of an organization that provides services and/or lodging and is identified by the CoC as part of its service system; A continuum project can be classified as one that provides lodging (lodging project) or one that does not provide lodging (services project). Also referred to as a **Program.**

Protected Health Information ("PHI") means any information, whether oral or recorded in any form or medium that is held or created by a Covered Entity or Business Associate and that:

1. Relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; and,
2. Identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and,
3. Is limited to the information created or received by BA from or on behalf of CE.

Protected Personal Information (PPI) - Any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

Personally, Identifying Information (PII)- Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.

Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

XII. Attachments

The attachments listed below can be found on the Blue Ridge Continuum of Care's website, which can be found at the following link: www.endhomelessnessblueridge.org. Will be added once policies are approved by BRICH.

The website includes the most up-to-date and recent version of all documents related to HMIS such as (but not limited to): Links will be added later. All documents are included below.

1. The HMIS Release of Information (ROI) - Click here
2. The Personal Protected Information Statement – Click here
3. The HMIS Data Collection Statement – Click here
4. The HMIS Password Policy – Click here
5. HMIS Vendor Disaster Recovery Summary Plan – Click here

XIII. Acknowledgements & Revision History

This HMIS Policy and Procedures Handbook was collaboratively written and informed by versions of other HMIS Policies and Procedures from other communities. This version was completed and approved by BRICH in _____ 2023

XIV. Appendix

HMIS Lead Agency
Council of Community Services
502 Campbell Ave SW
Roanoke, VA 24016

Tel: 540-266-7551 (CCS Main Office)
540-682-3005 (HMIS Lead Staff Person)
540-632-2109 (HMIS System Administrator)

Email: hmis@councilofcommunityservices.org

HMIS Help Desk:
https://forms.office.com/Pages/ResponsePage.aspx?id=zEEVAc97DEmLU8XCBGoqyvwgesQXgQVMkzuF-sckl0tUNFA0SjlPQkZFOEQ5T0wzTVNINkE4U0w0Si4u