South Carolina

Homeless Management Information System

Policies and Procedures

Revised and Approved by the South Carolina HMIS Steering Committee:

February 25, 2021

Table of Contents

SOUTH CAROLINA
HOMELESS MANAGEMENT INFORMATION SYSTEM
POLICIES AND PROCEDURES

This document defines the Policies and Procedures of the South Carolina (SC) Homeless Management Information System (HMIS). SC HMIS encompasses the four Continua of Care in South Carolina: Total Care for the Homeless Coalition (TCHC), Midlands Area Consortium for the Homeless (MACH), Upstate Continuum of Care (UCoC), Lowcountry Continuum of Care (LCoC), and the Statewide 2-1-1 Information and Referral line. This document has been approved by the respective organizations. All HMIS Users must be provided a copy and be familiar with this document. For reference on terminology, please refer to Appendix A: Definition of Terms.

This document was approved by a vote of all parties on February 25, 2021. As with any change in policy, it is not expected that all parties be in immediate retroactive compliance with the new policies described in this document – especially when previous practice was following guidance outlined in older versions of the Policy and Procedure Manual. The policies described in this document are to be adhered-to from February 25, 2021 forward.

1. Governance Structure

Policy: HMIS shall be governed by the primary decision-making body of the Continuum of Care (CoC). The primary decision-making body will appoint an HMIS Lead Agency. The HMIS Lead Agency, if different from the CoC, guides the implementation of the HMIS. However, the CoC is ultimately responsible for the HMIS. The CoC ensures participation of all qualified agencies in the HMIS. The CoC, if different from the HMIS Lead Agency, can designate the HMIS Lead Agency to assist in ensuring Memorandums of Agreement (MOA) are executed with all qualified Contributory HMIS Organizations (CHO). The CoC ensures that the HMIS is being carried out according to the guidelines set forth in this document and the HMIS Data and Technical Standards provided by the U.S. Department of Housing and Urban Development (HUD).

Procedure: The CoC's HMIS Lead Agency shall be responsible for selecting and designating the representative(s) to the South Carolina HMIS Steering Committee described below.

2. South Carolina HMIS Steering Committee

Policy: Primary decisions regarding the statewide HMIS implementation ("Community Services" from WellSky, formerly known as "ServicePoint") that affect all lead agencies (i.e. CoC, HMIS Lead Agency) are made by the South Carolina HMIS Steering Committee. The HMIS/211 Sharing Agreement, coordinated by the United Way of the Midlands (the contract holder), defines the Steering Committee and its responsibilities. Whenever updates are made to the Policy and Procedure Manual, these updates will need

to be presented to and approved by each CoC's Leadership Body (Advisory Council, Governing Board, etc…).

Procedure: As defined in the HMIS/211 Sharing Agreement, the South Carolina HMIS Steering Committee is comprised of at least one person designated by each HMIS Lead Agency and 211 Parties. It shall meet, as needed (typically on a bi-weekly basis), to make decisions regarding:

- Implementation / Training
- Expansion
- Project Management
- Oversight
- Enforcement
- Coordination
- Contracts
- Policies and Procedures
- Other Duties Related to the Governance of the Shared HMIS

The four Continuums of Care are expected to assume rotating leadership of the South Carolina HMIS Steering Committee by appointing a Committee Lead from within the CoC. The rotation will follow this order: MACH, Upstate CoC, Lowcountry CoC, TCHC (repeat). Meetings shall be called by the Committee Lead or at the request of any of the HMIS Lead Agencies. Meeting times and places are arranged by the Steering Committee Lead who will also chair all meetings. Meetings may be conducted by email, webinar, or telephone provided all participants agree.

When there is a vote to be had to accomplish committee work, each CoC will have one vote. The vote must carry at least three of the four votes. If there is a tie (2 CoC votes to 2 CoC votes), the vote would be opened to all members of the Steering Committee where each member would have a single vote. The tiebreaker would then be determined by a majority of the individual member votes.

3. Local CoC HMIS Committees

Policy: Each CoC shall designate a local committee ("HMIS Committee") to oversee the implementation of the HMIS and establish policies governing the HMIS within their local CoC. Policies must adhere to the guidelines set forth in this Policy and Procedure Manual and the HUD HMIS Data and Technical Standards. These local HMIS Committees make recommendations to the Steering Committee regarding:

- Implementation / Training
- Expansion
- Project Management
- Policies
- Oversight
- Enforcement
- Coordination
- Contracts

- Policies and Procedures

Procedure: The CoC or the HMIS Lead Agency ensures the establishment of the local HMIS Committee and that its responsibilities, activities, and progress are tracked and documented.

4. Contributory HMIS Organization

4.1. Contributory HMIS Organization (CHO)

Policy: Participation will be limited to Contributory HMIS Organizations (CHOs) providing housing and/or services to the homeless and those at risk of homelessness as defined by HUD.

First priority for participation as determined by the HMIS Standards is: (1) shelters – any facility with overnight sleeping accommodations where the primary purpose of which is to provide temporary shelter for the homeless in general or for specific populations of the homeless, (2) permanent housing providers servicing the homeless population, (3) service agencies targeting the homeless population, and (4) other agencies serving at-risk populations.

Domestic Violence and Victim Service Provider agencies are prohibited by HUD from participating in HMIS. DV agencies are instead either required or strongly encouraged to use a "comparable database" system that can produce de-identified required reports for funders while maintaining strict confidentiality of client-level data.

Procedure: All parties seeking to participate in the HMIS must contact the HMIS Lead Agency and provide information on the CHO and demonstrate ability to comply with the South Carolina HMIS Policies and Procedures. The subsequent step to participate in the HMIS is signing a Memorandum of Agreement (Appendix B).

Contact information for each HMIS Lead Agency (CoC in parens):

One80 Place (Lowcountry CoC): www.one80place.org
United Way of the Midlands (MACH): www.uway.org
Eastern Carolina Housing Organization (TCHC): www.echousing.org
United Housing Connections (Upstate CoC): www.unitedhousingconnections.org

4.2. Agreements to Participate

Policy: All Contributory HMIS Organization (CHO) in the HMIS must have a signed agreement with the HMIS Lead Agency. The HMIS Lead Agency must execute a Memorandum of Agreement (MOA; see Appendix B) to gain access to the HMIS. The MOA references the HMIS Standards that the partner agency must follow as a condition

for participation in the HMIS, including requirements for data collection, data quality, data sharing, privacy, and security. The MOA is to be used statewide by all for Continuums of Care – no other document can be substituted for the MOA.

Procedure: The MOA shall be approved in accordance with procedures of the Contributory HMIS Organization (CHO) and must be signed by the CHO Executive Director and an authorized official at the HMIS Lead Agency level.

4.3. Terms of Participation

Policy: The MOA includes: terms of participation; the disclosure of Universal Data Elements and additional local elements at least once annually; compliance with local, state, and federal laws with respect to data retention, transfer, use and disclosure; and defined responsibilities of all parties either explicitly or by reference to other documents.

Procedure: The terms of participation are outlined in the MOA. CHO signatures on the MOA represent agreement to the terms of participation. Approval of a CHO to participate in HMIS is at the discretion of the CoC.

As an additional term for participating in the HMIS, CHOs are prohibited from directly contacting the HMIS Vendor (WellSky) to request custom database work. Any such request must be made through the South Carolina HMIS Steering Committee via the local HMIS Lead Agency Staff.

4.4. HMIS Project Set-Up

Policy: Once the MOA has been signed, the CHO will work with the HMIS System Administrator to create the provider/providers under which client information will be collected and from which services will be rendered.

Procedure: The CHO must provide all the information requested by the HMIS System Administrator to complete project set-up. This information may include, but is not limited to:

1. Provider profile information
2. Standards information
3. Visibility requirements
4. Services provided
5. Module access settings
6. Assessments needed
7. Assessment display settings

Ideally, projects will be set-up in the HMIS before User access is granted.

4.4.1. Provider & Project Naming Convention

Policy: Specific projects operated under each provider will adhere to an established naming convention. This naming convention is shared across all four CoCs and helps to accurately convey the CoC where the project is located, and type of service provided by each project.

Procedure: Projects will follow the formula below when naming a project:

CoC HMIS Acronym – Project Name – Funding Source – Project Type

Each project's name will start with the acronym of the CoC it operates/provides services in:

LHC – Lowcountry Continuum of Care
MACH – Midlands Area Consortium for the Homeless
TCHC – Total Care for the Homeless Coalition
UHC – Upstate Continuum of Care

Next, the Project Name. This can be provided directly from the agency/provider running the project.

Next, a funding source can be included in the naming convention. This can help differentiate HMIS projects if two (or more) funding sources support the same project. For example, common homeless service funding sources are:

ESG: Emergency Solutions Grant
CoC: Continuum of Care Program
SSVF: Supportive Services for Veterans Families

Finally, the Project Type. The following abbreviations should be used:

ES: Emergency Shelter
RRH: Rapid Rehousing
PSH: Permanent Supportive Housing
TH: Transitional Housing
SO: Street Outreach
HP: Homelessness Prevention
SH: Safe Haven
SSO: Supportive Services Only
CES: Coordinated Entry System

A hypothetical example of a complete project name could be:

UHC–Hope for All–ESG–ES

5. Access to HMIS

5.1. Securing Access, Usernames, and Passwords

Policy: Access to the HMIS is restricted to only those with a valid User ID and password. Only a CHO that has signed the Memorandum of Agreement with the HMIS Lead Agency may apply for a User ID. All potential Users must receive training on the HMIS before an ID and password are provided.

User IDs may not be shared. The policy is one ID per User. No exceptions.

Procedure: The steps to obtain a valid User ID and password are:

1. CHO must have a signed MOA with the HMIS Lead Agency or HMIS Contractor. The individual User accessing the HMIS must be an employee, intern, or volunteer of the CHO.
2. CHO must request access to the HMIS for specific individual(s) through their HMIS Lead Agency.
3. CHO must select one or more individuals who will use HMIS and request training for those individuals. Each HMIS Lead Agency may develop policies on license allocation. The number of Users may be limited by the HMIS Lead Agency based on availability. Additionally, the HMIS Lead Agencies reserve the right to assess a fee per license based on availability or limited resources. There is no statewide policy in regards to license fees.
4. All new Users must complete training prior to access, which covers accessing Wellsky's Community Services (formerly known as "ServicePoint"), maintaining high data quality standards, and ensuring security/privacy. HMIS Lead Agencies reserve the right to assess fees for training. There is no statewide policy in regards to training fees.
5. Prior to training, each User must sign and initial the HMIS User Agreement (Appendix C). If required by the CoC, the form must also be signed by the User's immediate supervisor. Training will be provided by the HMIS Lead Agency or HMIS contractor providing the HMIS support for the Lead Agency.
6. If the CHO utilizes a subcontractor to enter client data, the CHO shall provide a copy of the subcontractor agreement and a written statement of their authorization to access the system on behalf of the CHO to the HMIS CoC Administrator. The HMIS User Agreement must be signed by the CHO, Executive Director of the subcontractor CHO, and system User.
7. Each User must read the HMIS Privacy Policy (Appendix D), HMIS Confidentiality Guidelines (Appendix E), and the HMIS Code of Ethics (Appendix F) prior to accessing the HMIS for the first time and to the extent reasonable, each User must sign an acknowledgement of having done so.

8. The CHO is responsible for informing its HMIS Administrator, if possible, prior to, but in any event, within 24 hours of: a staff member who is an HMIS User leaving his or her workforce status; termination of appropriate access to the HMIS by a subcontractor; or for other reasons any User should no longer have access to HMIS.
9. With any User ID, the User will be given a single-use, temporary password, which must be changed upon the User's first access to the HMIS. Passwords should be complex and unique; for example, passwords should be more than 8 characters, a mix of numbers and symbols, and avoid repeating letters/numbers. Passwords are the individual's responsibility and Users cannot share passwords. Users may not keep written copies of their password in a publicly accessible location. Any passwords that are written down are to be stored securely and must be inaccessible to other persons. Users are not to store passwords on a personal computer for easier log-in. Passwords expire every 45 days. Users may not use the same password consecutively. Passwords cannot be re-used until two password selections have expired. If a User unsuccessfully attempts to log-on three times, the system will force the User to reset their own password or have their password reset by the HMIS System Administrator.
10. A User will be at risk of losing their HMIS license after 30 days of non-use. CoCs reserve the right to terminate the license and/or charge an agency a penalty fee for non-use of the system at their discretion. There is no statewide policy in regards to charging agencies a non-use penalty fee.

5.2. User Conflict of Interest

Policy: Current clients, or volunteers who were clients receiving homeless services within the last six months, cannot be granted access to the HMIS. Former clients who have been hired by an agency to perform HMIS duties will be granted access with approval from the local HMIS Lead Agency. Additionally, all Users cannot modify client records for which an obvious conflict of interest exists.

Procedure: Current clients receiving homeless assistance/services or volunteers who have received homeless services within the past six months are not allowed to have User access to the HMIS. A period of six-months must pass from a volunteer's exit from a homeless assistance project before they may begin the process to secure User access to the HMIS. This reduces the potential for the former client to access personal information on persons they might have received services alongside, many of whom remain highly vulnerable while actively experiencing homelessness.

Former clients who have been hired (not serving on a volunteer basis) will be eligible for access to HMIS upon approval by the HMIS Lead Agency.

Users who have records in HMIS are prohibited from entering or editing information in their own record. All Users are also prohibited from entering or editing information in files of immediate family members.

All Users must sign the HMIS User Agreement, which includes a statement describing this limitation, and report any potential conflict of interest to their designated agency HMIS Contact. The System Administrator may run the audit report to determine if there has been a violation of the conflict of interest agreement.

5.3. Types of Users (User ID Privileges)

Policy:

Depending on the need and training level, HMIS Users may have different access to the data and functions of the HMIS. The HMIS defines four primary levels of User access:

1. **"Volunteer" –** Non-paid staff members of a CHO may be given Volunteer User IDs. This User ID enables client data input and shelter bed check-in and checkout only.

2. **"Case Manager"** – Most Users will be assigned a Case Manager User ID. This ID enables new client entry and exiting, data entry and editing of case notes and service transactions, and bed list check-in and check-out only. All Case Managers with a User ID within a CHO have complete access to all data entered by all other case managers and Volunteer Users within the CHO as well as most data entered and shared by another CHO.

   In the system, there are three levels of Case Manager access. Most all Case Manager level Users will have Case Manager III access which includes the following privileges: access to all modules except "Administration," view all screens within Client Point, view program data for all providers on the provider tree, and have access to run reports.

3. **"Agency Administrator"** – This User ID provides the same access rights as Case Manager, plus access to provider profiles. Users with this access level may assign and activate/deactivate User IDs, and may reassign temporary passwords for Users in their agency, and have additional authority to run reports on their agency for data quality assurance and performance monitoring. Agency Administrators may also create and delete flash news articles for their agency. Each coalition and large CHO (those with

more than 3 Users and at the discretion of the HMIS System Administrator) may request an Agency Administrator User ID.

4. **"System Administrator II"** – Users with this access level have complete access to all data records within the HMIS and to all administrative functions within the HMIS. Each HMIS Lead agency has one or more System Administrator II Users, and these individuals have access to provider profiles and all data entered by all individuals. System Administrator IIs should be an employee or contractor of the HMIS Lead Agency.

Procedure: A CHO must contact the HMIS Administrator of the HMIS Lead Agency to request training for potential new HMIS Users. The CHO must also specify the requested privileges of such potential User. The HMIS Administrator will ensure that training is consistent with the User level and need.

5.4. Violations and Non-Compliance Policy

Policy: Users are required to follow the Policies and Procedures defined in this document. If there are violations to this policy, Users and/or agencies will face repercussions.

Procedure: This Policy and Procedure Manual may be updated at any time. All Users will be kept informed of changes to this document by email, and the most recent version is always available on each CoC's website.

Lowcountry Continuum of Care: lowcountrycoc.org/
Midlands Area Consortium for the Homeless: www.midlandshomeless.com/
Total Care for the Homeless Coalition: https://tchcsc.org/
Upstate Continuum of Care: https://www.upstatecoc.org/

Failure to comply with these Policies and HMIS Lead Agency policies may result in the suspension or revocation of a User ID. In addition, any suspicion of unauthorized activity should be reported immediately to HMIS Lead Agency staff.

The South Carolina HMIS Violations and Non-Compliance Policy is listed in Appendix G. Each User and CHO must agree to abide by this Policy and follow its guidelines on how violations to the South Carolina HMIS Policy and Procedure Manual will be investigated and enforced.

6. Data

6.1. Ownership of Data

Policy: The CoC is the custodian of the data, and each CHO owns the client data it enters into the HMIS System, subject to applicable law and data rights as well as Section 6.2.2 below. If a CHO is inactive in HMIS or leaves the system for six consecutive months or permanently exits the system, ownership of the client-level data reverts to the CoC. However, as a partner in HMIS, each CHO agrees to share data with other organizations for referral and coordination of services. Data also may be shared with organizations outside of HMIS, pursuant to an executed Research Agreement (see Section 7.6 below) or with the SC Revenue and Fiscal Affairs Office (RFA) for research purposes.

Procedure: Data is stored on a server in a secure location at WellSky (see Section 8.4 below for more information). A backup of the complete South Carolina HMIS Community Services Database is provided on a weekly basis to United Way of the Midlands (UWM) - the contract holder for the shared system. This backup is held on the secure UWM server and is moderated by United Way of the Midlands IT staff. The back-up is overwritten on a weekly basis; historical back-ups are not held indefinitely.

6.2. Data Privacy

6.2.1. Privacy Statement

Policy: Each CHO must post a copy of the **Privacy Statement** (Appendix H) at each intake desk (or comparable location) which explains the reasons for collecting data and the general use and disclosure of such information.

Procedure: A CHO may not modify this statement or combine it with existing privacy statements.

6.2.2. Privacy Policy

Policy: Each CHO will abide by the HMIS Privacy Policy (Appendix D), which defines the privacy practices of all CHOs.

Procedure: Each CHO must have a copy of the HMIS Privacy Policy (included in Appendix D). The HMIS Privacy Policy cannot be modified in any form; each CoC must use the version of the Privacy Policy included in the most recent version of this Policy and Procedure Manual.

The Privacy Policy describes standards for the privacy of personal information collected and stored in the South Carolina Homeless Management Information System (SC HMIS), as well as personal information collected for the purposes of the Coordinated Entry Systems for the four Continuums of Care (SC CoCs) across the State of South Carolina. The standards seek to protect the confidentiality of personal information while

allowing for reasonable, responsible, and limited uses and disclosures of data. This Privacy Policy is based on principles of fair information practices recognized by the information privacy and technology communities. Uses and disclosures of client information are defined by the 2004 HMIS Data and Technical Standards Final Notice.

This Policy applies to any homeless assistance organization that records, uses, or processes personally identifiable information (PII) for the SC HMIS and/or the SC CoCs CES. A provider that meets this definition is referred to as a Contributory Homeless Organization (CHO).

A CHO may use or disclose PII only if the use or disclosure is allowed by this Policy. A CHO may assume consent for all uses and disclosures specified in this Policy and for uses and disclosures determined by the CHO to be compatible with those specified in this Policy. This Policy limits the disclosure of PII to the minimum necessary to accomplish the purpose of the disclosure. Uses and disclosures not specified in this Policy can be made only with the consent of the client or when required by law.

The HMIS Privacy Policy must be available for clients to access. If a client is illiterate, the CHO must ensure that a workforce member reads the HMIS Privacy Policy to the client to ensure the client is fully aware of privacy practices and the client's rights. The CHO must make reasonable accommodations for people with hearing impairment, visual impairment, cognitive impairment, and limited English proficiency. It is not advised to review the Privacy Policy with an individual who is impaired due to alcohol and/or substance use.

As a change from previous South Carolina HMIS Policy and Procedure directives, a Release of Information (ROI) is no longer required to be collected from the client to use or disclosure their information for purposes outlined in the Privacy Policy. However, clients may request their information not be shared with any other CHO participating in the HMIS. CHOs may request assistance from their CoC's HMIS System Administrator in regard to limiting the sharing of a client's data if they request it.

6.3. Merging Duplicate Client Records

Policy: In order to avoid duplicating client records, User

s should always search for an existing client record before creating a new client. In the event a User finds duplicate records for a client, the User should

submit a request to the HMIS Lead Agency for a System Administrator to address the merge.

Procedure: System Administrators should merge duplicate client records whenever a valid merge request is received. Requests should include all duplicate client ID numbers with an indication of which client ID number has correct demographic information that should be maintained.

In merging the client records, System Administrators should maintain the correct demographic information provided by the User. The final destination Client ID number should be the record with the lowest HMIS ID number, unless the record contains inaccurate information, in which case the system administrator should use his or her discretion.

During a client merge, if one of the clients originated in another CoC, the System Administrator from the CoC conducting the merge must contact the other System Administrator(s) from the other CoC(s) to let them know a merge needs to take place before the merge can be executed. This courtesy allows for communication about specific circumstances that should be addressed before the merge is finalized.

Once a merge is completed, it is recommended that the System Administrator send an email to each agency that had provided services to the client within the past three years so the agencies can update their records accordingly.

Locked records subject to unique security regulations required by the project's funding source (i.e. HIPAA, RHYMIS, HOPWA, PATH) should remain locked and cannot be merged. Older client records not subject to these regulations that were locked before transitioning to global visibility should be opened and merged.

HMIS Lead Agencies are responsible to conduct periodic reviews of potential duplicate client records and address those using the criteria listed above.

6.4. Other Data

Policy: A CHO may enter additional data on each client as it feels is useful and in compliance with these Policies and Procedures. Unneeded information, particularly if sensitive, should not be included.

Procedure: HMIS includes many assessment screens designed to collect additional data. The HMIS Lead Agency creates each CHO's set of assessment screens at the direction of the CHO. This is part of the process identified in Section 4.4 "Project Set-Up."

6.5. Data Quality, Accuracy, and Timeliness

6.5.1. Data Quality

Policy: The HUD HMIS Data Standards define specific data elements that must be collected and entered into HMIS. HUD defines two categories of data elements: *Universal Data Elements* - required to be collected from all homeless clients served by any CHO, and *Program Specific* data elements - collected from all clients if the CHO receives HUD grant funds (i.e. Continuum of Care, Emergency Solutions Grant, SSVF, RHY, PATH, and HOPWA).

Procedure: See Appendix J for the most recent HMIS Data Quality Plan. Not adhering to the guidelines specified in the HMIS Data Quality Plan can impact a CHOs performance monitoring evaluation. CoC's reserve the right to levy penalties or fines for not adhering to Data Quality standards.

6.5.2. Data Accuracy

Policy: Users must make their best efforts to obtain accurate and complete information. The most important data elements to enter are the full name, date of birth, and gender. Users may not intentionally enter invalid or incorrect data.

Procedure: Data is reviewed periodically by CHO Administrators and the HMIS Lead Agency for accuracy and completeness.

Reports are to be run at the discretion of the HMIS Lead Agency. Please see Section 3 of the 2020 HMIS Data Standards Manual for required Universal Data Elements and Section 4 for Program Specific Data Elements required by HUD. Not adhering to the data completeness policy of having 96% or above "non-null" data values can impact a CHOs performance monitoring evaluation. CoC's reserve the right to levy penalties or fines for not adhering to Data Accuracy standards.

6.5.3. Data Timeliness

Policy: The preferred method of data collection and entry is real-time with data being entered into HMIS as it is collected. When this is not possible or practical, data must be entered into HMIS within 72 hours of when the data is collected, but sooner if possible.

Procedure: Data timeliness reports showing number of clients with data entered more than a week after collection will be reviewed,

and any CHO with a significant number of late entries will be notified about additional training or corrective action. Not adhering to the data timeliness policy of entry <72 hours from collection can impact a CHOs performance monitoring evaluation. CoC's reserve the right to levy penalties or fines for not adhering to data timeliness standards.

6.6. Data Imports

Policy: Allowances of data imports into the HMIS will be limited and only approved by the SC HMIS Steering Committee.

Procedure: While HMIS databases are required to have the capacity to accept data imports, the SC HMIS Steering Committee reserves the right to not allow data imports into the South Carolina HMIS database. Allowing data imports will impact data quality and increase the likelihood of duplication of client files in the system.

6.7. Information Regarding Children

Policy: Whenever possible, the CHO should not receive information directly from a child under the age of 13 without the parent's express written consent.

Procedure: When a User collects information from a child under the age of 13, the CHO is obligated to: (1) provide notice regarding the information to be collected from children, how HMIS uses such information, and disclosure practices; (2) attempt to obtain verifiable (written) parental consent; (3) provide, upon the parent's request (if parent is contactable), a description of the specific personal information collected from the child; (4) cease collecting the child's personal information at the parent's request. The procedures and policies in this policy document protecting the confidentiality, security, and integrity of information will apply to all personal information of children.

6.8. Procedure to Follow if Approached by Law Enforcement for Client Information in HMIS

Policy: The CHO and User must contact the HMIS Administrator and CoC leadership (as defined locally by each Continuum of Care) whenever there is a request from Law Enforcement to access a client's information within the HMIS.

Procedure: The situation might arise where Law Enforcement requests access to a client's information recorded within the HMIS. If this occurs, the User and CHO who received the request must immediately contact the HMIS Administrator and the CoC

leadership about the request. The CoC leadership, in consultation with the CHO and the CHO's own policies on disclosure of personal information, will make a determination about the feasibility of the request and either approve or deny it. If the request from Law Enforcement is approved, then the CHO will be free to share the specific information requested (and no more) with Law Enforcement. If the request is denied, the CoC leadership will communicate directly with Law Enforcement about this determination and take future steps as needed.

7. Privacy and Security Plan

7.1. Device Security

Policy: WellSky Community Services, the software used for the HMIS, is accessed via the Internet. A broadband internet connection is necessary. To maintain security, computers used to access HMIS must be secured by a firewall. Both a hardware firewall (router) and a software firewall are required, as well as anti-virus and anti-spyware applications. Transmission of data will be secured according to the procedures below.

When Users work remotely, they are required to follow the SC HMIS Remote Access Guidelines included in Appendix K.

Procedure: The following standards apply to CHOs and HMIS Lead Agencies to ensure security for all devices on a network that is accessing HMIS:

A browser that supports 256-bit TLS encryption, such as Google Chrome, Internet Explorer 11, Microsoft Edge, or Mozilla Firefox. Internet browsers must be updated with the latest security updates available.

A vendor supported and updated operating system. These include Microsoft Windows 8/8.1/10 and Mac OS X v10.11.6 or newer. Operating systems must be kept updated with the latest security patches available.

All devices, including a single computer not on a network, must connect to the internet through a router. A modem that includes connections for more than one computer, but includes a router, is acceptable, otherwise a router must be added. Wireless networks should be secured with WPA2 security.

Each computer used to access HMIS must be protected by a personal firewall as well as anti-virus and anti-spyware software. Anti-virus/anti-spyware software must include an online service to keep it up to date, and the software must be kept current.

If a device used to access HMIS is on a network, all devices on the network must be protected as described above.

Devices used to access HMIS must be kept secured with an encrypted password. Device and HMIS account passwords must be unique, kept secured, and may never be shared with anyone. If a password is believed to be compromised it must be changed immediately.

7.2. Data Security

Policy: There are a number of state and federal regulations covering the release of client-identifiable data. The HUD HMIS Data and Technical Standards also specify minimum security requirements for the HMIS. Client identifiers include name, date of birth, and social security number, among others.

Procedure: The following protocols are to be followed to ensure the security of data entered into the HMIS:

1. All Users are issued a *unique* User ID and temporary password to access the system in accordance with Section 5.1 above.
2. All Users must sign confidentiality statements and attend training that includes information on data security.
3. Hard copies of data (if kept by the agency) must be stored in a locked file cabinet.
4. The HMIS Lead Agency shall be responsible for the destruction and disposal of its data, and each CHO shall be responsible for the destruction and disposal of its own data. Files must be disposed of appropriately in accordance with current industry standards after a minimum of 7 years, unless stored for research purposes (e.g., by cross-cut shredding of paper documents, magnetic swiping, and erasing and sanitizing electronic data in accordance with standards set out by the National Institute of Standards and Technology ("NIST")).
5. Computers must be set to lock after 10 minutes of inactivity and must be protected with a screen saver.
6. Computers are not to be left alone with PII data displayed.
7. After 3 failed log-in attempts, the User's password will be inactivated and they will be required to reset their password using the "Forgot Password" link in Community Services. Or, they may contact their System Administrator.
8. All data transmitted electronically must be encrypted (e.g., by encoding the data in such a way that only authorized parties can access it and those who are not authorized cannot).
9. Any data with PII stored on a device or external media (including removable devices, flash drives, and external hard drives) must be encrypted in accordance with the current industry standard.

7.3. Client Data Sharing

Policy:

The types of data, levels of sharing, and typical sharing settings are listed below. These criteria identify the standard levels of client data sharing allowed by this Policy and Procedure manual.

HMIS contains six types of data:

1. Client record
2. Household composition
3. Primary assessment data (data captured on the primary assessment page used by the CHO)
4. Client needs and services provided
5. Goals and case notes
6. Other assessment data not included in #3 above

We define three levels of data sharing:

- Shared globally (shared with all other Users on the HMIS). This is the default for all client data entered into the HMIS system and allowed for by the uses and disclosures covered the in the HMIS Privacy Policy.
- Shared selectively (as specified by the CHO working in conjunction with the HMIS System Administrator).
- Not shared.

Typical settings: The following are default settings that can be changed to address individual circumstances:

- Client record data (Name, SSN, Veterans Status) is shared globally to ensure Users are able to complete a Client Search to identify if a record exists in the HMIS for the client presenting for services.
- Household composition, assessments (primary or otherwise), and needs/services are shared globally or shared selectively (depending on the service provider collecting the data).
- All other data (including goals/case notes) is not shared. However, a CHO may request any specific assessment or group of data defined in HMIS to be shared, either globally or selectively.

ALL providers for mental health services or any CHO whose primary clients are children (defined as 17 years and below), or any CHO whose primary services are for HIV/AIDS or substance abuse, are set to only share Client record data.

Procedure:

The majority of provider profiles in the HMIS are set to share globally. Thus, all CHOs must provide the client access to the SC HMIS Privacy Policy, which explicitly states the purposes for which the CHO collects, uses, and discloses the data.

NOTE: The Systems Administrator(s) has access to ALL client data. This access is primarily used to provide technical support to Users. The HMIS Systems Administrator(s) are required to limit the use and disclosure of any protected health information to any individual or organization.

7.4. Client Record Information (Name, SSN, Veterans Status) on Client Profile Tab

Policy: In HMIS, Client record data is located on the Client Profile tab. For de-duplication purposes, this data is shared with all CHOs to ensure CHOs and Users are able to conduct a Client Search of the database to locate existing client records.

Procedure: The Client record data will be visible on the Client Profile Tab. However, no other assessments, or sub-assessments is to be visible on the Client Profile Tab. Client Profile tab is to be used strictly for de-duplication purposes.

7.5. Aggregate Data Sharing and Release

Policy: Reports generated by any CHO or the HMIS Lead Agency may be shared with another CHO and/or made public provided the report contains only aggregate data and is devoid of client identifiers. In nearly all circumstances, with few exceptions described below, client-level data will be reserved for the HMIS Lead Agency/CoC for research, planning, and Coordinated Entry System purposes.

Procedure: Reports that include any of the following information, or regarding which the disclosure of said information could be used to identify an individual, MAY NOT BE shared outside of HMIS or your agency with the exception of Revenue and Fiscal Affairs (RFA), via a signed Research Agreement (Appendix L) with an approved research organization or university (see Section 7.8), or as required by the Coordinated Entry System. The following are considered "identifiers":

- Names;
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (A) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (B) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- All elements of dates (except year) for dates directly related to an individual, including birth date, service date, date of death; and all ages over 89 and all elements of

dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code.

7.5.1. Release of Data for Grant Funders

Policy: Funding Agencies should not expect access to HMIS unless there is a MOA in place between the funder and the HMIS Lead Agency. The Lead Agency must then present this unique MOA agreement to the South Carolina HMIS Steering Committee for approval.

Procedure: Entities providing funding to agencies or programs required to use HMIS will not have automatic access to HMIS. Funder access to HMIS will only be granted by the South Carolina HMIS Steering Committee when there is a voluntary written Memorandum of Agreement in place between the funding entity and appropriate HMIS Lead Agency. Funding for any agency or program using HMIS cannot be contingent upon establishing a voluntary written agreement allowing the funder HMIS access.

7.5.2. Statewide Reporting

Policy: When aggregate statewide HMIS data is requested, all four CoCs must agree on the scope, data extraction/compilation, and review of the findings before the results are released.

Procedure: Data requests that include data for multiple CoCs will be submitted using individual CoC's data request portals. The CoC receiving the data request will bring the request to the South Carolina HMIS Steering Committee for discussion. The data request will then be reviewed by each CoC's HMIS lead, who

will provide a list of projects and/or parameters for their CoC that need to be considered for the report execution. Once the data is compiled, it will then be submitted to each CoC's HMIS Lead for review. CoCs will then have five business days from the date they receive the data to conduct their review and provide their feedback or approval. Once the approval has been given, the aggregate data will be provided to individual or organization that requested the information.

7.6. Data Extracts

Policy: General extracts (Excel worksheets, CSV or any other format) of data in HMIS may not be shared with any other agency or organization if it contains any client identifiers listed above in Section 7.5.

The exception to this policy is that extracted data with client identifiers may be shared with another organization for research purposes provided there is a Research Agreement (See Appendix L) in place between the third party and the HMIS Lead Agency. The Research Agreement requests in-depth information about the purpose of the proposed research, the qualifications of the researchers, and steps the researchers will take to protect the personal information provided. The CoC and HMIS Lead Agency reserve the right to review the research findings and, based on that review, potentially deny the release of findings. The Research Agreement also requires that client identifiers only be used to match information between data sources. After the data matching is completed, identifiable information will be removed from the dataset, and a new unique id will be created. Due to the sensitive nature and rare occurrences of these research agreements, each research agreement must be reviewed and approved by the South Carolina HMIS Steering Committee.

Additionally, extracts may be shared with HMIS affiliated CHOs for the purposes of compliance with HUD's required Coordinated Entry System, but must be sent in an encrypted format.

Procedure: To share data with a third party for the purpose of research and aggregate reports with data matched from other data sources, the HMIS Lead Agency must have a signed Research Agreement with the third party explicitly detailing the constraints of access to, reproduction of, and distribution of the data as outlined above. The research agreement must be reviewed by the HMIS Lead Agency and the South Carolina HMIS Steering Committee prior to signing.

8. System Support, Monitoring, Requirements, and Disaster Preparedness

8.1. Technical Support

Policy: The System Administrator II(s), CHO Administrators, or the designated technical assistance contact for the CoC shall provide technical support to agencies and Users as needed.

Procedure: Users should contact the HMIS Lead Agency or the designated HMIS technical assistance contact for the CoC via the communication method (e.g. ticketing system) established by each HMIS Lead Agency.

8.2. HMIS Monitoring

Policy: System Administrators will also have the right to conduct monitoring of agency and User compliance with the policies and procedures detailed in this document.

Procedure: A baseline "SC HMIS Monitoring Tool" of HMIS Requirements, Response (compliance), Assessment, and Action Items is included in Appendix M. This Checklist represents a baseline for what system administrators should consider when conducting HMIS monitoring. Each CoC reserves the right to add-on to this baseline tool (i.e. strengthening and adapting the tool to their own CoC's characteristics/needs), but do not have permission to remove any items being evaluated. CoC's also reserve the right to conduct their HMIS monitoring in accordance to locally-defined priorities as decided by their localized HMIS Committee or CoC leadership.

If the CHO does not pass their monitoring, a corrective action plan will be developed between the CHO and the HMIS Lead/HMIS Contractor. The corrective action plan is to be completed by the CHO within 90 days of the delivery of the corrective action plan from the HMIS Lead/HMIS Contractor.

The HMIS Lead Agency may periodically review CHO and User compliance with Policies and Procedures and assist, where practical, with technical support to help such CHO comply.

8.3. Vendor Requirements

Policy: The HMIS Vendor (WellSky) is obligated to maintain security, performance, and support of the database system. To meet these requirements, the vendor must comply with the following procedures.

Procedure: WellSky will comply with the following requirements to ensure optimal operation of the system.

Physical Security
Access to areas containing HMIS equipment, data and software will be secured.

Firewall Protection
The vendor will secure the perimeter of its network using technology from firewall vendors. Company system administrators monitor firewall logs to determine unusual patterns and possible system vulnerabilities.

User Authentication
Users may only access HMIS with a valid Username and password combination that is encrypted via SSL for internet transmission to prevent theft. If a User enters an invalid password three consecutive times, they are automatically shut out of that HMIS session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Application Security
HMIS Users will be assigned a system access level that restricts their access to appropriate data.

Database Security
Wherever possible, all database access is controlled at the operating system and database connection level for additional security. Access to production databases is limited to a minimal number of points; as with production servers, production databases do not share a master password database.

Technical Support
The vendor will assist HMIS staff to resolve software problems, make necessary modifications for special programming, and will explain system functionality to HMIS staff.

Technical Performance
The vendor maintains the system, including data backup, data retrieval and server functionality/operation. Upgrades to the system software will be continuously developed and implemented.

Hardware Disposal
Data stored on broken equipment or equipment intended for disposal will be destroyed using industry standard procedures.

8.4. Disaster Preparedness

Policy:

The HMIS software vendor provides disaster recovery services. The basic Disaster Recovery Plan includes the following (language provided directly from WellSky):

- Nightly database backups
- Offsite storage of backups
- 7-day backup history stored locally on instantly accessible RAID storage
- 1-month backup history stored off site
- 24 x 7 access to WellSky's emergency line to provide assistance related to "outages" or "downtime"
- 24 hours backed up locally on instantly-accessible disk storage

Standard Recovery: All customer site databases are stored online, and are readily accessible for approximately 24 hours; backups are kept for approximately one (1) month. Upon recognition of a system failure, a site can be copied to a standby server, and a database can be restored, and site recreated within three (3) to four (4) hours if online backups are accessible. As a rule, a site restoration can be made within six (6) to eight (8) hours. On-site backups are made once daily and a restore of this backup may incur some data loss between when the backup was made and when the system failure occurred.

All internal servers are configured in hot-swappable hard drive RAID configurations. All systems are configured with hot-swappable redundant power supply units. Our Internet connectivity is comprised of a primary and secondary connection with separate internet service providers to ensure redundancy in the event of an ISP connectivity outage. The primary Core routers are configured with redundant power supplies, and are configured in tandem so that if one core router fails the secondary router will continue operation with little to no interruption in service. All servers, network devices, and related hardware are powered via APC Battery Backup units that in turn are all connected to electrical circuits that are connected to a building generator.

All client data is backed-up online and stored on a central file server repository for 24 hours. Each night an encrypted backup is made of these client databases and secured in an offsite datacenter.

Historical data can be restored from backups as long as the data requested is 30 days or newer. As a rule, the data can be restored to a standby server within 6-8 hours without affecting the current live site. Data can then be selectively queried and/or restored to the live site.

For power outage, our systems are backed up via APC battery back-up units, which are also in turn connected via generator-backed up electrical circuits. For a system crash, Non-Premium Disaster Recovery Customers can expect six (6) to eight (8) hours before a system restore with potential for some small data loss (data that was entered between the last backup and when the failure occurred) if a restore is necessary. If the failure is

not hard drive related these times will possibly be much less since the drives themselves can be repopulated into a standby server.

All major outages are immediately brought to the attention of executive management. WellSky support staff helps manage communication or messaging to customers as progress is made to address the service outage. WellSky takes major outages seriously, understands, and appreciates that the customer becomes a tool and utility for daily activity and client service workflow.

Procedure: HMIS Lead Agencies and the South Carolina HMIS Steering Committee will monitor the HMIS implementation health and coordinate directly with WellSky in the case of unexpected outages or disaster-related impacts. As described in Section 6.1, a localized back-up of the database is held in possession of United Way of the Midlands (the contract holder). This back-up is curated by United Way of the Midlands IT staff.

Appendices

APPENDIX A: DEFINITION OF TERMS

DEFINITION OF TERMS

Client Profile – The tab in Community Services where primary client identifiers and demographic information are stored. These data include: name, date of birth, social security number, race, gender, and veteran status.

Client Record – The data elements of name, social security number, and veteran status are considered the Client Record. These data elements are what are used to conduct a client search and to create new clients in Community Solutions.

Continuum of Care or CoC – The primary decision-making entity defined in the funding application to HUD as the official body representing a community plan to organize and deliver housing and services to meet the specific needs of people who are homeless as they move to stable housing and maximum self-sufficiency.

Contributory HMIS Organization or CHO – An organization that operates a contributory homeless assistance program or homelessness prevention program or contributory non-homeless assistance program. Programs can be part of a CHO, or an organization can operate programs independent of a CHO. These programs contribute Personal Identifiable Information (PII) to the system.

Department of Housing and Urban Development or HUD - The Department of Housing and Urban Development is a part of the U.S. federal government that is responsible for policies that relate to providing housing.

HMIS Administrator or System Administrator – The person(s) who shall have complete control and access to all functions of the HMIS. All changes to the system that affect all Users on the system are coordinated and agreed upon by the HMIS Steering Committee and made by the respective HMIS CoC Administrators.

HMIS Lead Agency – An organization designated by a CoC to operate the CoC's HMIS on its behalf. The HMIS Lead Agency is in partnership with the CoC with a written agreement.

HMIS User Agreement – The agreement each User must complete and agree to before access to the HMIS can be granted. Upon signing this agreement and completion of required training, the User will be provided a User ID and temporary password.

HMIS Visibility Adjustment Instructions – Process for Users to follow when a client requests a restriction in data sharing/coordination across the HMIS implementation.

Homeless Management Information System or HMIS - The information system designated by a CoC to process Personal Identifiable Information (PII) and other data in order to create an unduplicated accounting of homelessness within the CoC. HMIS may provide other functions beyond unduplicated accounting. The HMIS database includes information on client records, services needed and provided, shelter bed stays, case notes, and case plans.

HUD HMIS Data and Technical Standards – The federal notice with guidelines governing an HMIS. All CHO's using an HMIS must comply with the most recent *HMIS Data Standards, and HMIS Technical Standards of US Department of Housing and Urban Development, Office of Community Planning and Development*.

Lowcountry Continuum of Care or LCoC – The Lowcountry Continuum of Care plans, develops and implements comprehensive and coordinated strategies to address homelessness in Beaufort, Berkeley, Charleston, Colleton, Dorchester, Hampton, and Jasper Counties in South Carolina.

Memorandum of Agreement or MOA – A signed agreement between the CHO and HMIS Lead Agency that includes specific requirements the CHO must follow to gain and maintain access to the HMIS. The MOA must be executed between the Grantee and all participating agencies. The documents must be signed by the Executive Director of the CHO.

Midlands Area Consortium for the Homeless or MACH – The Midlands Area Consortium for the Homeless was formed in the early 1990's as a grassroots organization to advocate for funding to address homelessness. Through collaboration, MACH has grown to include over 50 partner members throughout 13 counties in the Midlands of South Carolina. For more than 20 years, MACH has been helping individuals obtain stable housing and employment and education necessary to become self-sufficient.

Participant – A South Carolina Continuum of Care or its designated HMIS Lead Agency or 2-1-1 call center that has signed the HMIS Sharing Agreement.

Privacy Policy – A policy that describes standards for the privacy of personal information collected and stored in the South Carolina Homeless Management Information System (SC HMIS), as well as personal information collected for the purposes of the Coordinated Entry Systems for the four Continuums of Care (SC CoCs) across the State of South Carolina.

Privacy Statement – A notice that must be placed at the point of intake and posted on the CHO's website. When posted, consent of the individual may be inferred depending on the circumstances of the collection of data.

Program Data Elements – Those data elements listed by HUD as "Program Data Elements."

Personal Identifiable Information or PII – Any information maintained by or for an organization about a 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 data to identify a specific individual. The HUD HMIS Standards lists: Name, SSN, Date of Birth (DOB), and Zip Code of last permanent address, program entry and exit dates, and any unique internal identification number generated from any of these items as PII. PII must have special protections to ensure that casual observers do not have access to this data. See Section 8.7 for a list of identifiers.

Research Agreement – Document that must be agreed to by the South Carolina HMIS Committee and a third party such as a University or research organization before client-level information will be provided. The Research Agreement details the purpose of the study, information about who will be conducting the research, security measures taken, and intended publications/products to be produced by the research.

SC Revenue and Fiscal Affairs or RFA – State-sponsored research organization that maintains a data warehouse on various human services. Research partnerships with RFA have historically been used to develop an understanding of the efficacy of homeless services across the state.

South Carolina HMIS Steering Committee – The governing body of the statewide South Carolina HMIS implementation. The Steering Committee is responsible for the development and enforcement of the HMIS Policy and Procedure Manual.

South Carolina HMIS Code of Ethics – A set of guiding principles for the CHO and Users of the HMIS**.**

South Carolina Interagency Council on Homelessness or SCICH – A statewide network of advocates, service providers, and funders committed to ending homelessness in South Carolina.

Statewide HMIS Violations and Non-Compliance Policy – Document that provides guidelines on how violations to the South Carolina HMIS Policy and Procedure Manual will be investigated and enforced.

Total Care for the Homeless Coalition or TCHC – The Total Care for the Homeless Coalition works to break the cycles of homelessness experienced by individuals and families in the 13 northeastern counties of South Carolina: Chesterfield, Clarendon, Darlington, Dillon, Florence, Georgetown, Horry, Kershaw, Lee, Marion, Marlboro, Sumter, and Williamsburg.

Universal Data Elements – The data elements listed by HUD as "Universal Data Elements."

Upstate Continuum of Care or UCoC – The Upstate CoC is a community of individuals and providers that organize and deliver housing and services to individuals experiencing homelessness as they move to stable housing and maximum self-sufficiency. Serving 13 counties in Upstate, SC, the Continuum of Care aims to prevent, reduce, and end homelessness through the coordination of agencies in our communities.

User – An employee, volunteer, affiliate, associate, and any other individual acting on behalf of the CHO or HMIS Lead Agency who uses or enters data into the HMIS or another administrative database from which data are periodically uploaded to the HMIS and who has been appropriately assigned a User ID in accordance with Section 5.1 and who qualifies for access to the HMIS in accordance with these Policies and Procedures.

Victim Service Provider or VSP – A private nonprofit organization whose primary mission is to provide direct services to victims of domestic violence.

WellSky's Community Services (formerly known as ServicePoint) – The software product upon which the South Carolina Homeless Management Information System implementation operates.

APPENDIX B: MEMORANDUM OF AGREEMENT

HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

MEMORANDUM OF AGREEMENT

between

(CoC Acronym)

and

Potential New Agency

THIS AGREEMENT made and entered into this**, (DATE OF AGREEMENT)** by (Name of **Potential New Agency),** and between (Name of CoC followed by the **CoC Acronym),** the collaborative applicant for the Department of Housing and Urban Development Continuum of Care Homeless Management Information System (HMIS) on behalf of the **(NAME OF CoC)** hereinafter called the Continuum of Care ("CoC") and (NAME OF **Potential New Agency),** hereinafter called the CHO (Contributory HMIS Organization). This organization operates a contributory homeless assistance program or contributory non-homeless assistance program, to assist with funding of an electronic data collection system that stores longitudinal personal level information about persons who access the homeless services system in the CoC. (COC ACRONYM) is the HUD recognized CoC for the (specific CoC region), known to HUD as (specific CoC location code.) The system allows CHOs to input and share information concerning people experiencing homelessness and those clients at risk of homelessness. The system is supported by federal funds from the U.S. Department of Housing and Urban Development, hereinafter called "HUD."

WITNESS THAT:

WHEREAS, (CoC Acronym) received funding from HUD under its Continuum of Care Program to assist the CoC in operating the Homeless Management Information System (HMIS) through which services are documented, tracked, reporting accomplishments accurately and without duplication of effort, resulting in client service delivery improvements within the (COC ACRONYM) CoC's region; and

WHEREAS, HMIS is a web-based information management system that provides client tracking and case management, service and referral management, bed availability for shelters, reporting, and is capable of supporting all applicable service providers (COC ACRONYM) within the CoC, plus other South Carolina regional areas; and

WHEREAS, (CoC Acronym) has accepted the responsibility of administering federal and local matching funds to meet HUD Continuum of Care Program guidelines and maximizing program benefits to all HMIS staff and consultants; and

WHEREAS, the CHO provides coordinated entry system, shelter, housing, and supportive services for individuals and families; and

WHEREAS, the signature of the Executive Director of the CHO signifies the CHO's concurrence with, and
acceptance of, the terms of this agreement before the creation of an account for the CHO on HMIS.

NOW, THEREFORE, valuable consideration and mutual promises hereafter set forth between the parties hereto, the legal sufficiency of which is hereby acknowledged by the parties, it is agreed as follows:

I. SCOPE OF SERVICES FOR (CoC Acronym). As part of the HMIS, (CoC acronym) agrees to act as the grantee, and in partnership with the CoC to be the custodian of the data, to:

A. Provide support of the ServicePoint™ HMIS application from WellSky, with the mutual goals of collaboration, enhanced service delivery, and comprehensive data collection; plus, the inclusion of User license(s) licensing, disaster recovery, training, project management, annual support, and security via its ServicePoint HMIS vendor. For further detailed about WellSky's data security practices, please refer to the appendix of this MOA.

B. Maintain and Manage the HMIS providing leased hosting of the ServicePoint system on a WellSky server as the centralized database for all client information.

C. Provide HMIS Components based on agency needs at the discretion of (CoC Acronym). Components may include User license(s), consulting services (Assessment, Training, and Support)

D. Privacy Policy and Statement Documentation. The South Carolina HMIS Privacy Policy and Privacy Statement must be used explicitly as it is provided in the most recent version of the HMIS Policy and Procedure Manual. No other versions of these documents are allowed to substitute for the approved Privacy Policy and Privacy Statement.

E. Provide HMIS Training. (CoC Acronym) and the CHO agree that training is mandatory to all End Users. (CoC Acronym) will be responsible for providing training, which will be determined by the HMIS System Administrator.

F. Provide HMIS Technical Support. All requests for technical support shall be forwarded to the (CoC Acronym) ticketing system.

II. SCOPE OF SERVICES FOR CHO. As part of the HMIS, the CHO, as the owner of the data, agrees to:

A. Provide, at a minimum, the data elements required by HUD, CoC, and other federal grants to generate an unduplicated count.

B. Provide data to facilitate the sharing of information for research initiated by the CoC.

C. Assist the (CoC Acronym) in meeting the baseline HMIS standards for data collection, data quality, privacy, and security as outlined in the HMIS Policies and Procedure Manual Adhere to all HUD HMIS Guidance

D. Enter data promptly to ensure information generated by the HMIS presents an accurate picture of people accessing the homeless services system within the CoC.

E. Work Closely With the (COC ACRONYM). CHO agrees to cooperate fully with (COC ACRONYM) in providing data and information to support the HMIS.

F. Appoint Personnel. CHO agrees to designate User(s) and assumes the responsibility for

its staff and System Users' compliance with data entry requirements, including but not limited to preventing entry of inappropriate and duplicate client records, inaccurate information, or entry of client records that are missing required data elements. The CHO will ensure all new System Users complete and execute Attachment B and are provided with training before accessing the HMIS. The CHO will, as soon as practicable but in no event to exceed 48 hours, notify (COC ACRONYM) in writing of any new, released, or terminated personnel.

G. Attend Training**.** CHO agrees to attend any mandatory HMIS Training/User Group meetings provided by (COC ACRONYM).

H. Actively participate in the HMIS. CHO agrees to make its best effort to utilize the HMIS to the fullest extent practicable with the CHO's plan and to provide community support.

I. Maintain updated virus protection on agency hardware and User license(s) that access the HMIS.

J. Refrain from transmitting material in violation of any Unites States federal or state law or regulation including, but not limited to, copyright materials, material legally judged to be threatening or obscene, and material considered protected by trade secret.

K. Refrain from using the HMIS to defraud the federal, state or local government or an individual entity, or to conduct any illegal activity.

III. PRIVACY AND CONFIDENTIALITY. The HMIS will include client identifier information (name, date-of-birth, and social security number). The HMIS may include, but not be limited to, information required by HUD relating to disabilities and special needs, which can include HIV/AIDS, substance abuse, mental illness, physical or medical disability, developmental disability, and domestic violence. Social and caseworker notes and comments may also be contained within the HMIS. There are strict federal and state privacy rules regarding this and any other medical data in a client's record (See Attachment). All CHOs must maintain a Privacy Policy and post the HMIS Privacy Statement by the HMIS Policies and Procedures.[1]

1. Protection of Client Privacy

1. The CHO will comply with all applicable federal and state laws regarding the protection of client privacy, including, but not limited to, Federal confidentiality regulations as contained in the *Code of Federal Regulation, 42 CFR part 2,* regarding disclosures of alcohol and drug abuse records.

2. Confidentiality of information about client data is a high priority for (COC ACRONYM) and the CHO. Users must be trained by (COC ACRONYM) System Administrator before accessing the HMIS. Training will include instructions related to client privacy and confidentiality as well as for instructions on using the HMIS.

3. (COC ACRONYM) reserves the right to suspend without notice services of the HMIS for investigation of any suspicion of breached confidentiality.

4. (COC ACRONYM) may suspend this agreement if CoC, in its sole discretion, determines that there has been an improper breach of confidentiality.

5. The CHO will comply with all HUD and HMIS Policies and Procedures established by the (COC ACRONYM).

6. If the CHO is covered under HIPAA, it is not required to comply with the privacy and security standards in the HMIS Policy and Procedure Manual. If the CHO determines that a substantial portion of its PII about homeless clients is protected health information as defined by HIPAA, they are to follow the HIPAA guidelines on data privacy and security.

IV. TERM AND PERFORMANCE

A. The MOA shall remain unless revoked in writing by either party with 30 days written notice or until HUD discontinues funding for grants and any subsequent renewals to it.

B. (COC ACRONYM) shall provide licensing, technical support, training, and implementation cost as part of the grant agreement with HUD. (CoC) may entirely or partially cover license costs.

C. If, at the time, funding is discontinued from HUD, the CHO is responsible for operating and maintenance costs necessary to continue the operation of its proportional share of the HMIS.

D. If (COC ACRONYM) terminates this agreement for any reason other than for convenience under Section IV. A hereto, the CHO shall surrender any User license (s) provided under this agreement. The CHO shall immediately refrain, as of the effective date of termination, from using the HMIS. Except for terminations for convenience under Section IV.A, the CHO has the right to appeal any termination to the (COC ACRONYM) Board.

E. Upon termination of this agreement for any reason, all client-level data will be retained within

HMIS for research and planning purposes.

V. NOTICES

- Official communication concerning this agreement shall be directed to:

  1. (CoC Acronym)

VII. MONITORING

A. (COC ACRONYM) shall conduct periodic monitoring and reviews of the CHO to ensure compliance with this agreement and the HMIS regulations. The areas reviewed may include, but are not limited to, data quality, the operation of the User license (s), maintenance and enforcement of confidentiality procedures, and reporting functionality, if applicable.

B. If monitoring or review reveals deficiencies in the CHO's compliance with HMIS regulations or performance under this agreement, the discovery of such deficiency, (COC ACRONYM) shall develop and provide to the CHO a written plan of correction as outlined in the Monitoring Tool.

C. Should CHO fail to satisfy the terms of the Monitoring Tool findings, (COC ACRONYM) may, at its sole discretion, terminate this agreement as outlined in the Monitoring Tool.

VIII. TERMS AND CONDITIONS OF THIS AGREEMENT

A. This agreement, by 24 CFR 85.43, may be suspended or terminated if the CHO materially fails to comply with any term of the agreement, and that the agreement may be terminated for

convenience by 24 CFR 85.44.

B. It is understood and agreed between the parties that (COC ACRONYM) is in no way connected with the actual performance of the services to the clients facilitated by this agreement on the part of the CHO, nor as to the employment of labor or the incurring of other expenses. Nothing in this Agreement shall be construed to be inconsistent with the CHO's status an independent contractor or construed to constitute the CHO, or any of its agents or employees as agents, employees or representatives of (COC ACRONYM). The CHO will supervise the execution of all work covered by the agreement which shall be in the exclusive charge and control of the CHO.

C. Subject to the terms and conditions of this Agreement, (COC ACRONYM) will provide an HMIS System Administrator and provide training and technical support for the HMIS as needed if there are HUD grant funds to cover support of the HMIS.

D. The CHO agrees to indemnify and to hold (COC ACRONYM), its employees, officers, and agents harmless from any claims for damages to persons and/or property arising out of or in any way connected with the performance of any work, services or functions covered by this agreement and the use by the CHO of the HMIS. (COC ACRONYM) agrees to indemnify and hold the CHO and all valid Users of the HMIS harmless from any claims for damages to persons and property arising out of or in any way connected with the use of the HMIS to the extent permitted by law. The CHO agrees that as an independent contractor, it will not assert in any legal action by claim or defense or take the position in any administrative procedures that it is an agent or employee of (COC ACRONYM).

E. This agreement cannot be transferred by assignment or novation, nor shall any of the work covered by such agreement be subcontracted without the prior written approval of (COC ACRONYM), which may be granted or withheld in its sole discretion. In the event of an unauthorized assignment, novation, or attempt to subcontract services, this agreement shall be void.

F. This Agreement can only be amended only upon the mutual written consent of the parties.

G. The CHO shall always, comply with all laws, regulations, and ordinances governing the performance of the services described herein.

H. The waiver by either party of a breach or violation of any provision of this agreement shall not operate as nor be construed to be a waiver of any subsequent breach thereof.

I. This document contains the entire agreement between the parties, and no statement or representation not contained herein shall be valid.

IX. ATTACHMENTS

Attachments to the Memorandum of Agreement are included throughout this Appendix section of the Policy and Procedure Manual. For a standalone version of the MOA including all attachments, please contact your CoC HMIS Administrator

APPENDIX C: HMIS User Agreement

HMIS User Agreement

This certification must be completed by all new and existing Users on an annual basis. If you have any questions, please contact the HMIS Manager:

Lauren Hopkins - MACH HMIS Manager
803-733-5101
lhopkins@uway.org

Please complete the following information:

Agency Name:

Employee Name & Position Title: _____

Employee Email Address: _____

Employee Contact Number: _____

USERS RESPONSIBILITIES/PROCEDURES

- Each User requires a unique Username and private password. The use of another User's Username and/or password or account is grounds for immediate termination of participation in the HMIS (removal of all access for all Users).
- A User ID and temporary password will be assigned and emailed to the User once this form is completed and returned to the local CoC HMIS System Administrator.
- After reviewing the Confidentiality Guidelines **(Appendix E)** please sign the Confidentiality and Responsibility Certification **(next page)**

HMIS USER AGREEMENT
CONFIDENTIALITY AND RESPONSIBILITY CERTIFICATION

Access to the HMIS will be used only for legitimate client services and administration of the agency listed below. Any breach of confidentiality will result in immediate investigation by the HMIS Lead Agency and potential termination of access to the HMIS.
Initial each item:

____ I understand that my Username and password are for my use only.

____ I understand that I must take all reasonable means to keep my password physically secure. Specifically, passwords are not to be left on or near the computer or my desk.

____ I understand that the only individuals who can view data within the HMIS are authorized Users, though clients may be provided information about themselves contained in HMIS.

____ I understand that I may only view, obtain, disclose, or use the database information that is relevant and necessary in performing my job.

____ I understand that these rules apply to all Users of HMIS whatever their role or position.

____ I understand that hard copies of HMIS data must be kept in a secure file.

____ I understand that once hard copies of HMIS data are no longer needed, they must be appropriately destroyed to maintain confidentiality.

____ I understand that if I notice or suspect a security breach I must immediately notify the local CoC HMIS System Administrator.

____ I understand that I may not intentionally enter incorrect data.

____ I will notify the appropriate local HMIS System Administrator within 24 hours of termination of employment.

____ I agree to avoid any conflict of interest (see Section 5.2 of the HMIS P&P Manual) when viewing or editing client information within HMIS.

____ I have read and understand the HMIS Confidentiality Guidelines.

____ I have read and understood the HMIS Privacy Policy.

____ I have read and understood the HMIS Code of Ethics.

I have read, understand, and agree to the Confidentiality Guidelines above.

Employee's Signature	Date
Supervisor's Signature	Date
CoC HMIS System Administrator Signature	Date

South Carolina HMIS Privacy Policy

This Policy describes standards for the privacy of personal information collected and stored in the South Carolina Homeless Management Information System (SC HMIS), as well as personal information collected for the purposes of the Coordinated Entry Systems for the four Continuums of Care (SC CoCs) across the State of South Carolina. The standards seek to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data. This Privacy Policy (hereinafter referred to as "Policy") is based on principles of fair information practices recognized by the information privacy and technology communities.

This Policy defines the privacy standards that will be required of any organization within the State of South Carolina that records, uses, or processes personally identifiable information (PII) on clients at-risk of or experiencing homelessness for the SC HMIS, and/or the CoCs CES process. Organizations must also comply with federal, state, and local laws that require additional confidentiality protections, where applicable.

This Policy recognizes the broad diversity of organizations that participate in the SC HMIS and/or the CES processes, and the differing programmatic and organizational realities that may demand a higher standard for some activities. Some organizations (e.g., such as non-VSPs serving victims of domestic violence) may choose to implement higher levels of privacy standards because of the nature of the clients they serve and/or service provision. Others (e.g., large emergency shelters) may find higher standards overly burdensome or impractical. At a minimum, however, all organizations must meet the privacy standards described in this Policy. This approach provides a uniform floor of protection for clients at-risk of or experiencing homelessness with the possibility of additional protections for organizations with additional needs or capacities.
The following sections discuss the South Carolina Continuums of Care Privacy Policy (SC HMIS Privacy Policy).

I. SC CoCs Privacy Policy: Definitions and Scope

a. Definition of Terms

i. *Personally Identifiable Information (PII):* Any information maintained by or for a Contributory Homeless Organization about a client at-risk of or experiencing homelessness 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.

ii. *Contributory Homeless Organization (CHO):* Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses, or processes PII on clients at-risk of or experiencing homelessness for an HMIS or CES. This definition includes both organizations that have direct access to the SC HMIS and/or the SC CoCs CES, as well as those organizations who do not but do record, use, or process PII.

iii. *Processing:* Any operation or set of operations performed on PII, whether by automated means, including but not limited to collection, maintenance, use, disclosure, transmission, and destruction of the information.

iv. *HMIS and CES Uses and Disclosures:* The uses and disclosures of PII that are allowed by this Policy.

v. *Uses and Disclosures:* Uses are those activities internal to any given CHO that involves interaction with PII, whereas disclosures are those activities in which a CHO shares PII externally.

II. Applying the South Carolina HMIS Privacy Policy

This Policy applies to any homeless assistance organization that records, uses, or processes personally identifiable information (PII) for the SC HMIS and/or the SC CoCs CES. A provider that meets this definition is referred to as a Contributory Homeless Organization (CHO).

Any CHO that is covered under the Health Insurance Portability and Accountability Act (HIPAA) is not required to comply with this Policy if the CHO determines that a substantial portion of its PII about clients at-risk of or experiencing homelessness is protected health information as defined in the HIPAA rules. Exempting HIPAA-covered entities from this Policy avoids all possible conflicts between the two sets of rules.

This Policy gives precedence to the HIPAA privacy and security rules because:

1) The HIPAA rules are more finely attuned to the requirements of the health care system.
2) The HIPAA rules provide important privacy and security protections for protected health information; and
3) Requiring a homeless provider to comply with or reconcile two sets of rules would be an unreasonable burden.

It is possible that part of a homeless organization's operations may be covered by this Policy while another part is covered by the HIPAA standards. A CHO that, because of organizational structure, legal requirement, or other reason, maintains personal information about a client at-risk of or experiencing homelessness that does not fall under this Policy (e.g., the information is subject to the HIPAA health privacy rule) must describe that information in its privacy notice and explain the reason the information is not covered. The purpose of the disclosure requirement is to avoid giving the impression that all personal information will be protected under this Policy if other standards or if no standards apply.

III. Allowable HMIS and CES Uses and Disclosures of Personally Identifiable Information (PII)

Client consent for any uses and disclosures defined in this section is assumed when organizations follow HUD HMIS Standards for notifying clients of privacy policies (see 2004 HMIS Data and Technical Standards Final Notice in footer and Appendix A of this document).

A CHO may use or disclose PII from the SC HMIS, and/or the SC CoCs CES under the following circumstances:

1) To provide or coordinate services for an individual or household.
2) For functions related to payment or reimbursement for services.
3) To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions.
4) When required by law.
5) For research and/or evaluation; or
6) For creating deidentified PII.

CHOs, like other institutions that maintain personal information about individuals, have obligations that may transcend the privacy interests of clients. The following additional uses and disclosures recognize those obligations to use or

share personal information by balancing competing interests in a responsible and limited way. Under this Policy, these additional uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with this Policy). However, nothing in this Policy modifies an obligation under applicable law to use or disclose personal information.

Uses and disclosures required by law. A CHO may use or disclose PII when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law.

Uses and disclosures to avert a serious threat to health or safety. A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PII if:

1) The CHO, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and
2) The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

Uses and disclosures about victims of abuse, neglect or domestic violence. A CHO may disclose PII about an individual whom the CHO reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority (including a social service or protective services organization) authorized by law to receive reports of abuse, neglect or domestic violence under the following circumstances:

1) Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law.
2) If the individual agrees to the disclosure; or
3) To the extent that the disclosure is expressly authorized by statute or regulation; and the CHO believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PII for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

A CHO that makes a permitted disclosure about victims of abuse, neglect or domestic violence must promptly inform the individual that a disclosure has been or will be made, except if:

1) The CHO, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
2) The CHO would be informing a personal representative (such as a family member or friend), and the CHO reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as determined by the CHO, in the exercise of professional judgment.

Uses and disclosures for academic research or evaluation purposes. A CHO may use or disclose PII for academic research or evaluation conducted by an individual or institution that has a formal relationship with the CHO, if the research / evaluation is conducted either:

- By an individual employed by or affiliated with the research / evaluation entity where the research / evaluation project is conducted under a written research / evaluation agreement approved in writing by a program administrator (other than the individual conducting the research / evaluation) designated by the CHO or
- By an institution for use in a research / evaluation project conducted under a written research / evaluation agreement approved in writing by a program administrator designated by the CHO.

A written research / evaluation agreement must:

1) Establish rules and limitations for the processing and security of PII during the course of research / evaluation.
2) Provide for the return or proper disposal of all PII at the conclusion of the research / evaluation.
3) Restrict additional use or disclosure of PII, except where required by law; and
4) Require that the recipient of data formally agree to comply with all terms and conditions of the agreement.

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

Any research / evaluation on the nature and patterns of homelessness (at the CoC-wide or system-wide level) that uses PII HMIS data will take place only on the basis of specific agreements between researchers and the entity that administers the HMIS. These agreements must be approved by the Executive Committee(s) of the Board(s) of Director(s) for the applicable CoC(s) and must reflect adequate standards for the protection of confidentiality of data. *Disclosures for law enforcement purposes.* A CHO may, consistent with applicable law and standards of ethical conduct, disclose PII for a law enforcement purpose to a law enforcement official under any of the following circumstances:

- In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena.
- If the law enforcement official makes a written request for protected personal information that:
  - Is signed by a supervisory official of the law enforcement organization seeking the PII.
  - States that the information is relevant and material to a legitimate law enforcement investigation.
  - Identifies the PII sought.
  - Is specific and limited in scope to the extent reasonably practicable considering the purpose for which the information is sought; and
  - States that de-identified information could not be used to accomplish the purpose of the disclosure.
- If the CHO believes in good faith that the PII constitutes evidence of criminal conduct that occurred on the premises of the CHO:
- In response to a verbal request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PII disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics; or

- If the official is an authorized federal official seeking PII for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others); and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

IV. Privacy Requirements

All CHOs involved with the SC HMIS and/or the SC CoCs CES must comply with the privacy requirements described in this Notice with respect to:

1) Data collection limitations.
2) Data quality.
3) Purpose and use limitations.
4) Openness.
5) Access and correction; and
6) Accountability.

A CHO must comply with federal, state, and local laws that require additional confidentiality protections. All additional protections must be described in the CHO's privacy notice. A CHO must comply with all privacy protections in this Notice and with all additional privacy protections included in its privacy notice, where applicable. A CHO may maintain a common data storage medium with another organization (including but not limited to another CHO) that includes the sharing of PII. When PII is shared between organizations, responsibilities for privacy may reasonably be allocated between the organizations. Organizations sharing a common data storage medium and PII may adopt differing privacy policies as they deem appropriate, administratively feasible, and consistent with this Policy, which allows for the de-duplication of clients at-risk of or experiencing homelessness at the CoC level.

V. Collection Limitation

A CHO may collect PII only when appropriate to the purposes for which the information is obtained or when required by law. A CHO must collect PII by lawful and fair means and, where appropriate, with the knowledge of the individual. A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information (Privacy Statement). Consent of the individual for data collection may be assumed when the Privacy Statement is properly displayed according to this Policy.

VI. Data Quality

PII collected by a CHO must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PII entered into SC HMIS should be accurate, complete, and timely, as defined by the SC HMIS Data Quality Monitoring Plan (Appendix J of the SC HMIS Policies & Procedures). A CHO must develop and implement a plan to dispose of, or remove identifiers from, PII that is not in current use seven years after the PII was created or last changed (unless a statutory, regulatory, contractual, or other requirement mandates longer retention).

VII. Purpose Specification and Use Limitation

A CHO may use or disclose PII only if the use or disclosure is allowed by this Policy. A CHO may assume consent for all uses and disclosures specified in this Policy and for uses and disclosures determined by the CHO to be compatible with those specified in this Policy. This Policy limits the disclosure of PII to the minimum necessary to accomplish the purpose of the disclosure. Uses and disclosures not specified in this Notice can be made only with the consent of the client or when required by law.

A CHO processing PII for the purposes of the SC HMIS, and/or the SC CoCs CES will agree to additional restrictions on the use or disclosure of the client's PII at the request of the client, where it is reasonable to do so. This can include, but is not limited to, the following additional restrictions:

1) Entering client PII into the SC HMIS so that it is not shared with any other CHO; or
2) Using de-identified client information when coordinating services through the SC CoCs CES processes.

A CHO, in the exercise of professional judgment, will communicate with a client who has requested additional restrictions, when it is reasonable to agree to these and alternatives in situations where it is not reasonable. CHOs may also request assistance from their CoC's HMIS System Administrator regarding limiting the sharing of a client's data if they request it.

VIII. Openness

A CHO must adhere to this Policy describing its practices for the processing of PII and must provide a copy of this Policy to any individual upon request. If a CHO maintains a public web page, the CHO must post the current version of this Policy on the web page. A CHO must post the South Carolina CoCs Client Privacy Statement stating the availability of this Policy to any individual who requests a copy.

This Policy may be amended at any time and amendments may affect PII obtained by a CHO before the date of the change. An amendment to this Policy regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.

In addition, CHOs 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. See HUD Limited English Proficiency Recipient Guidance published on December 18, 2003 (68 FR 70968).

IX. Access and Correction

In general, a CHO must allow an individual to inspect and to have a copy of any PII about the individual. A CHO must offer to explain any information that the individual may not understand. A CHO must consider any request by an individual for correction of inaccurate or incomplete PII pertaining to the individual. A CHO is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information.

A CHO may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PII:

1). Information compiled in reasonable anticipation of litigation or comparable proceedings.
2) Information about another individual (other than a health care or homeless provider)
3) Information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or
4) Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

A CHO can reject repeated or harassing requests for access or correction. A CHO 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 PII about the individual.

X. Accountability

A CHO must establish a procedure for accepting and considering questions or complaints about this Policy. A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign a confidentiality agreement that acknowledges receipt of a copy of this Policy and that pledges to comply with this Policy.

Appendix A of the Privacy Policy

This appendix addresses special considerations for Runaway and Homeless Youth (RHY) Program and Youth Homelessness Demonstration Program (YHDP) service providers, per the RHY Program HMIS Manual.

I. No Consent Required for Data Collection

Data collection is the process of collecting and entering information into the SC HMIS and/or the SC CoCs CES by RHY or YHDP program staff. All RHY and YHDP projects are required to collect specific data elements, including the HUD Universal Data Elements and program-specific data elements for the RHY- funded or YHDP-funded project(s) for which they receive funding (Street Outreach Program, Basic Center Program, Transitional Living Program, Host Home, Permanency Navigator, etc.).
The Runaway and Homeless Youth Act requires that a RHY grantee "keep adequate statistical records profiling the youth and family members whom it serves (including youth who are not referred to out-of- home shelter services)."
RHY and YHDP grantees are not required to obtain youth or parental consent to collect and enter youth data into the SC HMIS, and/or the SC CoCs CES.

II. Consent Needed for Data Sharing

Data sharing refers to the sharing of client information per the Policy as laid out in this document. For RHY and YHDP grantees, data can only be shared if written consent is obtained from the parent or legal guardian of a youth who is under age 18, or with written consent from a youth who is 18 or older. HUD has clarified that the RHY Act is applicable for both RHY and YHDP grantees.

The RHY rule states the following regarding data sharing:
Pursuant to the Act, no records containing the identity of individual youth served by a Runaway and Homeless Youth grantee may be disclosed except:

1) For Basic Center Program grants, records maintained on individual youth shall not be disclosed without the informed consent of the youth and parent or legal guardian to anyone other than another organization compiling statistical records, or a government organization involved in the disposition of criminal charges against the youth.
2) For Transitional Living Programs, records maintained on individual youth shall not be disclosed without the informed consent of the youth to anyone other than an organization compiling statistical records.
3) Research, evaluation, and statistical reports funded by grants provided under section 343 of the Act are allowed to be based on individual youth data, but only if such data are de-identified in ways that preclude disclosing information on identifiable youth.
4) Youth served by a Runaway and Homeless Youth grantee shall have the right to review their records; to correct a record or file a statement of disagreement; and to be apprised of the individuals who have reviewed their records.
5) The Department of Health and Human Services (HHS) policies regarding confidential information and experimentation and treatment shall not apply if HHS finds that state law is more protective of the rights of youth.
6) Procedures shall be established for the training of RHY program staff in the protection of these rights and for the secure storage of records. 45 CFR § 1351.21.

III. Special Consideration for RHY-Funded and YHDP-Funded Programs

In consideration of the guidance laid out in the RHY Program HMIS Manual, RHY-funded and YHDP- funded grantees shall enter data into the SC HMIS, and/or the SC CoCs CES for youth served and seeking services that will not be shared with any other CHO, unless the grantee receives written consent from the youth or parent/legal guardian of the youth served that allows the disclosure of the youth's PII for the permissible purposes laid out in this Policy.

CONFIDENTIALITY GUIDELINES

The CHO agrees to abide by all present and future federal and state laws and regulations relating to the collection, storage, retrieval, and dissemination of client information for SC HMIS. The CHO will only release general client information (NOT including alcohol or drug abuse, HIV/AIDS, or mental health) with implied consent where client has been informed of the SC HMIS Privacy Policy and has been offered a copy. CHO will only release client confidential information that includes alcohol or drug abuse, HIV/AIDS, or mental health issues with **written** consent of the client. Federal laws include, but are not limited to, the federal confidentiality regulations as contained in the Code of Federal Regulations, 42 CFR Part 2., regarding the disclosure of alcohol and/or drug abuse record: The Health Insurance Portability and Accountability Act of 1996 (HIPAA), when applicable.

I. The CHO will only collect Protected Personal Information that is relevant to the HMIS and to its program operations and to comply with regulations governing the HMIS.

II. The CHO will provide a verbal explanation of the HMIS to clients and arrange, when possible, for a qualified interpreter, and/or make responsible accommodations for persons with disabilities to include sign language, braille, audio, or larger type. **Note: This obligation does not apply to CHOs who do not receive federal financial assistance and who are also exempt from the requirements of Title III of the Americans with Disabilities Act because they qualify as "religious entities" under that Act.**

III. The CHO will make a copy of the SC HMIS Privacy Statement available to any client requesting a copy.

IV. The CHO agrees to limit access to information furnished by the HMIS to its own employees specifically for the purpose of inputting or verifying client data and/or entering into the system records of services provided.

V. The CHO agrees to use due diligence and care in assigning staff to use HMIS. All such employees will be required to sign a statement of confidentiality, which includes a pledge of compliance (**Appendix C**). Each statement of confidentiality will be forwarded to and maintained by the System Administrator. The User ID of the person who is entering information is a part of the computer record. The CHO will verify that the person is authorized to enter data into the system.

VI. The CHO shall be responsible for the maintenance, accuracy, and security of all its homeless assistance records and terminal sites and for the training of agency personnel regarding confidentiality.

VII. The CHO Executive Director must accept responsibility for the validity of all records entered by the agency. The Executive Director may designate an immediate subordinate staff member with supervisory responsibilities for verifying the accuracy of information.

CODE OF ETHICS

As an employee or volunteer of a CHO of the SC Homeless Management Information System (HMIS) I will:

Agree to abide by all policies and procedures of the HMIS as stated in the most recent version of the SC HMIS Policy and Procedure Manual.

Agree to abide by all present and future federal and state laws and regulations relating to the collection, storage, retrieval, and dissemination of client information for the HMIS.

Agree to only collect Protected Personal Information that is relevant to the HMIS and to comply with the policies and procedures governing the HMIS.

Agree to limit access to information furnished by the HMIS to its own employees specifically for the purpose of inputting or verifying client data and/or entering into the system records of services provided.

Agree to be responsible for the maintenance, accuracy, validity, and security of all the homeless assistance records and terminal sites utilized for the purpose of inputting and/or updating information into the HMIS.

Agree to immediately notify the HMIS CoC Administrator of any suspected security beach.

Agree to make a copy of the HMIS Privacy Statement available to any client requesting a copy.

Agree to complete and provide updates of all required documents for system use.

Agree to ensure information entered is valid to the best of my knowledge.

Agree to declare conflicts of interest in relation to the HMIS and take appropriate action.

Agree not to discuss information entered within the HMIS in settings outside of the agency or Continuum of Care activities (such as for Coordinated Entry System purposes).

HMIS Lead Agencies reserve the right to immediately suspend HMIS usage and agreements when any terms of this Code of Ethics are violated or are suspected to be violated. This infraction and non-compliance process is spelled out in the SC HMIS Violations and Non-Compliance Policy.

South Carolina Statewide HMIS Violations and Non-Compliance Policy

HMIS Operating Policies Violation

HMIS Users and Contributory Homeless Organizations (CHOs) must abide by all HMIS operational policies and procedures found in the South Carolina Homeless Management Information System Policies and Procedures manual and the Request for HMIS User Account (Appendix C). Repercussion for any violation will be assessed in a tiered manner. Each User or CHO violation will face successive consequences – the violations do not need to be of the same type in order to be considered second or third violations. HMIS staff from the CoC's Lead Agency will determine the level of infraction. User violations do not expire. No regard is given to the duration of time that occurs between successive violations of the HMIS policies and procedures as it relates to corrective action. Violations of these policies and procedures will have potential negative impacts on an agency's ability to maintain CoC support for future funding opportunities (e.g. ESG and CoC/HUD funding). Each CoC also reserves the right to require agencies to pay for licenses (instead of receiving them for free) if they continue to incur violations to the HMIS Policy and Procedure Manual.

First Violation – the User and CHO will be notified of the violation in writing by their respective HMIS staff from the CoC Lead Agency. The User's license will be suspended for 30 days, or until the CHO notifies the HMIS staff of action taken to remedy the violation. Each CoC throughout the statewide implementation will provide necessary training to the User and/or CHO to help ensure the violation does not continue. The respective HMIS staff will then notify the South Carolina HMIS Steering Committee of the violation during the next scheduled meeting following the violation.

Second Violation – the User and CHO will be notified of the violation in writing by their respective HMIS staff from the CoC Lead Agency. The User's license will be suspended for 30 days. The User and/or CHO must take action to remedy the violation; however, this action will not shorten the length of the license suspension. If the violation has not been remedied by the end of the 30-day User license suspension, the suspension will continue until the CHO notifies the HMIS staff of the action taken to remedy the violation. The HMIS staff will provide necessary training to the User and/or CHO to ensure the violation does not continue. The respective CoC HMIS staff will then notify the SC HMIS Steering Committee of the violation during the next scheduled meeting following the violation.

Third Violation – the User and CHO will be notified of the violation in writing by their respective HMIS staff from the CoC Lead Agency. The respective HMIS staff will immediately suspend their license and notify the SC HMIS Steering Committee of the violation. The User's license will remain suspended until the SC HMIS Steering Committee makes a determination whether or not to terminate the license. If the SC HMIS Steering Committee determines the User should retain their User license, the respective CoC HMIS staff will provide necessary training to the User and/or CHO to ensure the violation does not continue. If the SC HMIS Steering Committee determines the User's license should be revoked, the license will be terminated, and the User account disabled. If Users who retain their license after their third violation have an additional violation, that violation will be immediately reviewed by the SC HMIS Steering Committee, likely leading to termination of the license.

Notifying the HMIS Staff of a Violation

It is the responsibility of the Agency Administrator or general Users at CHOs that do not have an Agency Administrator to notify HMIS staff in writing when they suspect that a User or CHO has violated any HMIS operational agreement, policy, or procedure. A complaint about a potential violation must include the User and CHO name, and a description of the violation, including the date or timeframe of the suspected violation. Complaints should be sent in writing via e-mail or postal mail to the HMIS System Administrator at the CoC where the violation occurred. The name of the person making the complaint will not be released by HMIS staff if the individual wishes to remain anonymous.

Investigating the Violation

Once the HMIS staff from the CoC Lead Agency have been contacted about an alleged violation, the HMIS staff will begin investigating the violation by collecting evidence and testimony from the parties involved. Higher importance will be placed on objective evidence of the infraction (such as audit reports) than subjective evidence (verbal or written testimony). After the evidence has been compiled, the violation will be considered by the appropriate level of oversight based on the level and frequency of violation (First and Second Violation: HMIS Staff, Third Violation: SC HMIS Steering Committee). The User and CHO will be notified in writing once a decision has been determined. If the User is found to have violated the HMIS operational policies, the appropriate penalties will be levied as described above. The investigation will be treated as confidential; nobody outside of the HMIS staff and those involved in the investigative process will be made aware of the ongoing investigation. However, the outcome of the investigation will be available from HMIS staff upon request, but not shared publicly unless deemed necessary by the HMIS staff.

Appeals Process

If a User or CHO is determined to have violated the HMIS operational policies and procedures, the User or CHO has the right to appeal this verdict with their CoC's highest level of leadership (i.e. the Advisory Council) within two weeks of being notified about their violation. The User must submit their appeal in writing to their CoC's highest-ranking leader (i.e. the Chair of the Advisory Council). The highest-ranking leader of the CoC then reserves the right to convene a council of CoC Leaders to hear verbal arguments from the User/CHO submitting the appeal and the CoC HMIS Staff. If any of the persons composing the council has any direct link to the User/CHO accused of the violation, resulting in a clear conflict of interest, then the individual(s) must recuse themselves from the council hearing the appeal. This council will then decide the outcome of the appeal. The decision of the council on this matter is final; there will be no other opportunity for appeal.

Violations of Local, State or Federal Law

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

Multiple Violations within a 12-Month Timeframe

During a 12-month calendar year, if there are multiple Users (three or more) with multiple violations (two or more) from one CHO, the CHO as a whole will be subject to the consequences listed under the Third Violation above. These frequent violations will also have potential negative impacts on their ability to maintain CoC support for future funding opportunities (e.g. ESG and CoC/HUD funding). Each CoC also reserves the right to require agencies to pay for licenses (instead of receiving them for free) if they continue to incur violations to the HMIS Policy and Procedure Manual.

Example HMIS Violations

A violation is defined as any action that directly contradicts a stated policy/procedure included in the SC HMIS Policies and Procedures Manual. Below are some examples of potential common violations of the HMIS policies and procedures. By no means is this an exhaustive list; violations will be determined on a case-by-case basis:

A. Sharing of HMIS Usernames and passwords
B. Writing down an HMIS User password and leaving it visible in a public place
C. Verbal or written sharing of personal identifying information (PII) to non-related organizations (including news/media)
D. Sharing of reports that include a client's name, date of birth, and/or SSN to any organization outside of the agency without appropriate approvals
E. Accessing HMIS from an unsecure internet-service provider
F. Consistently not adhering to the Policy and Procedure Manual guidance on data quality, timeliness, and accuracy.
G. Leaving HMIS open on your computer terminal while away from desk for 10+ minutes where there is a high likelihood non-system Users can view/access the system
H. Not informing local HMIS Admins about employees who leave their employment or should no longer have access to HMIS within a 24-hour timeframe from learning the employee no longer needed access to the system
I. Not having the approved HMIS Privacy Statement displayed in a public place as specified in the HMIS Policy and Procedure Manual

User Consent:

I have read the HMIS Violations and Non-Compliance Policy and agree to abide by the policy state above. I understand that if it is determined I have violated the policies outlined in the SC HMIS Policies and Procedures Manual, I will be subjected to the sanctions and/or corrective action outlined above. I also acknowledge that I have the right to appeal the sanction and/or corrective action as specified in the Appeals Process section. Any questions about these policies should be directed to the CoC HMIS System Administrator.

User's Signature: _____ Date: _____

Supervisor's Signature: _____ Date: _____

CoC HMIS System Administrator Signature: _____ Date: _____

HMIS Violations and Non-Compliance Policy
Complaint Form

Name of Person Submitting the Complaint: _____

Date of the Complaint Submitted (Today's Date): _____

Confidentiality Preference (Circle One):

I prefer to submit this complaint anonymously *I consent to being identified as the source of the complaint*

Written Statement:

Provide a written statement detailing the alleged violation of the HMIS Policy and Procedure Manual; including who committed the violation and how a specific policy and procedure (or multiple policies and procedures) was/were violated:

I certify that the statements provided on this Complaint Form are accurate and true:

Signature: _____ Date: _____

Email and/or mail this Complaint Form to your CoC's HMIS System Administrator

HMIS Violations and Non-Compliance Policy
Notice of Violation

Name of Individual and/or Agency Accused of a Violation: _____

If Individual, Agency of the Individual: _____

Date of Violation Notification: _____

Written Statement:

Provide a written statement about the complaint levied against you:

Based on the statement above, an investigation into these claims will proceed within the next 10 business days.

I certify that the statements provided on this Notice of Violation are accurate and true:

Signature: _____ Date: _____

CoC HMIS System Administrator

Email and/or mail this Notice of Violation to the individual who is accused of the violation and their agency's leadership. Please direct inquiries about this letter to your CoC's HMIS System Administrator

HMIS Violations and Non-Compliance Policy
Notice of Sanction

Name of Individual and/or Agency Sanctioned: _____

If Individual, Agency of the Individual: _____

Outcome of Investigation: **Sanctioned** **Not Sanctioned**

Level of Violation (Circle): **First Violation,** **Second Violation,** **Third Violation**

Date of Sanction Notification: _____

Written Statement of Sanction:

Provide a written statement that details the reasons this individual and/or agency is being sanctioned and the specific consequences or corrective action being levied:

I certify that the statements provided on this Notice of Sanction are accurate and true:

Signature: _____ Date: _____

CoC HMIS System Administrator

Email and/or mail this Notice of Sanction Form to the individual who committed the violation and their agency's leadership. Please direct inquiries about this letter to your CoC's HMIS System Administrator

HMIS Violations and Non-Compliance Policy
Appeals Form

Name: _____

Agency: _____

Date of Violation Complaint Filed: _____

Date of Violation Notification: _____

Date of Sanction Notification: _____

Date of Appeal (Today's Date): _____

Written Statement:

Please provide a written statement that details your reasons for appealing the sanction imposed:

I certify that the statements provided on this Appeals Form are accurate and true:

Signature: _____ Date: _____

Please email or mail this Appeals Form to your CoC's Highest Ranking Leader (i.e. Chair of the Advisory Council)

HMIS Violations and Non-Compliance Policy
Outcome of Appeals

Name: _____

Agency: _____

Was Appeal Heard by Council (Select One)? Y / N

If Heard, Outcome of Appeal (Selected One): Sanction Repealed Sanction Upheld

Written Statement:

Provide a written statement that details the reasoning why the sanction was either repealed or upheld. Also, provide a written statement on the enforcement or repeal of consequences originally levied in the sanction.

I certify that the statements in this Outcome of Appeal Form are accurate and true:

Signature: _____ Date: _____

CoC's Highest Ranking Leader (Chair of the Advisory Council)

Email and/or mail this Outcome of Appeal Form to the individual who committed the violation and their agency's leadership. Please direct inquiries about this letter to your CoC's Highest Ranking Leader (i.e. Chair of the Advisory Council)

PRIVACY STATEMENT

SUMMARY OVERVIEW	This organization provides services for individuals and families at risk of or experiencing homelessness. This organization participates in the South Carolina Homeless Management Information System (SC HMIS) and/or the four Continuums of Care's Coordinated Entry System (CES). The SC HMIS is used to collect basic information about clients receiving services from this organization. This requirement was enacted to get a more accurate count of individuals and families experiencing homelessness, and to identify the need for different services. The SC CoC's CES is used to connect individuals and families at risk of or experiencing homelessness to the services they need. This organization only collects information that is considered appropriate and necessary. The collection and use of all personal information are guided by strict standards of privacy and security. This organization may use or disclose information from the SC HMIS and / or the SC CoC's CES under the following circumstances: • To provide or coordinate services for an individual or household; • For functions related to payment or reimbursement for services; • To carry out administrative functions; • When required by law; • For research and / or evaluation; or • For creating deidentified data.
USES, RISKS, PROTECTIONS	• Information you provide to this organization will be entered into the HMIS and shared with partner organizations unless you opt-out. • You will receive the same services, whether you allow your personal information to be entered in the HMIS and shared with partner organizations or not. • Your personal information that is in the HMIS will not be shared with any other people or organizations outside of HMIS unless you say it can be. • Your personal information that is in the HMIS will not be shared with any other government organizations except as required by law. • Personally Identifying Information (PII), such as names, birthdays, and social security numbers, will be available to partner organizations in the HMIS for seven years. • Although careful measures are taken to protect the personal information entered in the HMIS, it may be possible that a person could access your information and use the information to locate you, commit identity theft, or learn about sensitive personal information entered in the HMIS. • Your data is protected by legal agreements signed by Users of the HMIS and by electronic encryption of your personal information.
YOUR RIGHTS & CHOICES	• You have the right to refuse to provide personal information, or to stop this organization from entering and sharing your personal information into the HMIS. • You have the right to change your mind about allowing this organization to enter and share your information into HMIS. You must notify this organization in writing if you change your mind. • You have the right to request a copy of the complete SC HMIS Privacy Policy, which describes in detail allowable uses and disclosures of data collected for the purposes of the SC HMIS and/or the SC CoC's CES.
CONTACT INFORMATION	Midlands Area Consortium for the Homeless (MACH) Continuum of Care 1818 Blanding Street, Columbia, SC 29201 Lauren Hopkins, HMIS Manager 803-733-5101 • lhopkins@uway.org midlandshomeless.com

HMIS DATA QUALITY PLAN

HMIS Data Quality Plan Overview:
The following are policies and procedures the CoC will implement to ensure the data integrity of agencies/programs. This brief overview provides a structure for each of the four South Carolina CoCs to maintain their own high level of data quality. Each CoC is expected to have their own Data Quality Plans that they train Users to adhere to while they use and input data into the HMIS.

Policy: CHO will provide the following levels of data accuracy, completeness, and timeliness:

- All names will be accurate to the best extent possible
- Nulls, data not collected, or 'unknown' entries in required data fields will not exceed 5%
- All Users should aim to have 0% null/data not collected data
- All services documented in the system will be compatible with the standard services provided by the project and required by the funding sources (if applicable)

Procedure: The HMIS Administrator(s) will perform regular data integrity checks on the HMIS system. Any patterns of error at a CHO will be reported to the Agency Administrator and/or User. When patterns of error have been discovered, Users will be required to correct data entry and will be monitored for compliance.

1.) The HMIS Administrator(s) shall generate data reports showing clients with missing Universal Data Elements and clients with missing Program-Specific Data Elements.
2.) The HMIS Administrator(s) will generate reports and submit to the Agency Administrator or User detailing data quality issues and timelines for correction.
3.) The HMIS Administrator(s) reports will inform targeted outreach made to agencies/Users specifying corrections that need to be made with clients who have data quality issues.
4.) The HMIS Administrator(s) can also generate custom reports to assist with data quality.
5.) The HMIS Administrator(s) can rerun reports for errant agencies/programs and follow up with the CHO leadership, if necessary.
6.) The data is to be corrected within 14 calendar days from initial notification and reviewed to make sure corrections are made appropriately.

Users can monitor their own data by running pre-program reports within ServicePoint. Helpful reports that most every User has available to them include: APR/CAPER Reports, Clients Served Reports or Daily Bed Reports. These reports help agencies to independently ensure a high level of data quality and integrity.

SC HMIS Remote Access Guidelines

Below are sections drawn from the SC HMIS Policy and Procedure Manual reminding you of your duties to assure data security while accessing and utilizing the HMIS database away from your work office. As a general reminder, *do not access HMIS from a Public WiFi connection* (meaning do not use HMIS at any place/location that a password is not required). See additional guidance below:

From Sections 7.1 Device Security & 7.2 Data Security:

The following standards apply to Contributor Homeless Organizations (i.e. HMIS-affiliated agencies), their end-users, and HMIS Lead Agencies to ensure security for all devices on a network that is accessing HMIS:
A browser that supports 256-bit TLS encryption, such as Internet Explorer. Internet browsers must be updated with the latest security updates available.

A vendor supported and updated operating system. These include Microsoft Windows 8/8.1/10 and Mac OS X v10.11.6 or newer. Operating systems must be kept updated with the latest security patches available.

All devices, including a single computer not on a network, must connect to the internet through a router. A modem that includes connections for more than one computer, but includes a router, is acceptable, otherwise a router must be added. Wireless networks should be secured with WPA2 security.

Each computer used to access HMIS must be protected by a personal firewall as well as anti-virus and anti-spyware software. Anti-virus/anti-spyware software must include an online service to keep it up to date, and the software must be kept current.

If a computer used to access HMIS is on a network, all computers on the network must be protected as described above.

Devices used to access HMIS must be kept secured with an encrypted password. Device and HMIS account passwords must be unique, kept secured, and may never be shared with anyone. If a password is believed to be compromised it must be changed immediately and your HMIS Administrator notified.

All data transmitted electronically must be encrypted (e.g., by encoding the data in such a way that only authorized parties can access it and those who are not authorized cannot).

Any data with PII stored on a device or external media (including removable devices, flash drives, and external hard drives) must be encrypted in accordance with the current industry standard.

Computers must be set to lock after 10 minutes of inactivity, must be protected with a screen saver, and require a password to be entered to unlock the computer.

Computers are not to be left alone with PII data displayed.

If you have any questions about this guidance, please contact your CoC-specific HMIS Administrator

SC HMIS COMMITTEE RESEARCH AGREEMENT

Conducting research on homeless services is a productive way to further advance the provision of homeless assistance. The purpose of this Research Agreement is to collect required information about potential research partnerships between the four South Carolina Continuums of Care and relevant third-party research organizations or Universities. This Agreement must be completed in-full by the research organization or University requesting access to client-level information from the South Carolina HMIS database. The SC HMIS Steering Committee will collectively review and provide formal approval of these requests. Note: a fee structure may be assessed based on the extent of the time/resources required to fulfill the approved request.

A. Application Information

Today's Date:	
Contact Name:	
Job Title:	
Organization:	
Address:	
Phone Number:	
Email Address:	
Alternate Contact Name: (if applicable w/ phone and/or email address)	
Title of Study or Report:	
Purpose of Study: Please include a statement of the reason(s) for requesting access to homeless client records or data.	
Benefits of Study: Please specify who is expected to benefit when detailing benefits.	
Description of Study or Report: Please include a description of your research question as well as sampling procedures, measurement plan including measurement instruments, analysis plan and procedures, informed consent, and time frame for completion of the study.	(You may attach a supplemental document or type a description below)
Professional Qualifications: Please include all members of your research team if applicable	(You may attach your curriculum vitae or resume)

IRB Approval (If applicable)	
Timeline: Please include timeline for the study including when you need homeless client data	
Use of Client Identifiers: I agree to the following Statement: The use of client identifiers will be limited to the sole purpose of creating a unique id for the client record for the purpose of matching this client with clients with the same identifier from other data sources. The data with client identifiers cannot be reproduced in any form, and it must be deleted once its purpose of data matching is complete.	I Agree _____ Initials I Do Not Agree: _____ Initials (Note: Application will be Denied)

B. Data Request

Please specify data elements requested and time periods for data you are requesting	

C. Intended Uses of Data

Describe any intended uses of the data or additional plans for release of the data.	Note: SC HMIS Steering Committee request an opportunity to read Publications and/or Reports and/or Presentations prior to publication and/or presentation.

D. Security and/or Confidentiality Measures

Describe what methods will be used to physically secure the data.	
Describe what methods will be used to electronically secure the data.	

E. Additional Requests

Please specify any additional assistance requested including reviewing and commenting on results or findings or narrative needed for your report.	

F. Financial Information

Please provide information on your financial support of either the South Carolina Interagency Council on Homelessness (SCICH) and/or the four South Carolina Continuums of Care (CoC) during his current year (not individual member agencies).	

G. Membership

Is your organization a member in good standing of the SCICH and/or the four South Carolina CoC's?	

G. Final Agreements

The Researcher agrees to not use data for other purposes beyond the scope of this Research Agreement without the written approval of the South Carolina HMIS Committee.	I Agree _____ Initials I Do Not Agree: _____ Initials (Note: Application will be Denied)
The researcher agrees to acknowledge the South Carolina HMIS Committee's assistance in publications/products that are produced via this Research Agreement	I Agree _____ Initials I Do Not Agree: _____ Initials (Note: Application will be Denied)

Signature of Lead Researcher/Requester:

_____ Date: _____

Signed Research/Data Applications should be emailed to the
Chair of the SC HMIS Steering Committee

For SC HMIS Steering Committee Use Only:

Request Approved:

Yes ___ No ___ Date Approved: __ - __ - ____

APPENDIX M: South Carolina HMIS Monitoring Tool

Monitoring Tool Begins on the Next Page

South Carolina HMIS Monitoring Checklist

Date: _____ Agency: _____ Monitor(s): _____

Monitoring is conducted on all agencies that participate in the Homeless Management Information Systems (HMIS) to ensure that agencies are taking the necessary precautions to ensure that client data is always secure and protected. If an agency is found deficient and does not pass the monitoring exercise, a corrective action plan will be provided by the HMIS Lead/HMIS Contractor. The corrective action plan must be addressed within 90 days of receipt.

Requirements	Description	2=Fully Met/Yes	1=Partially Met/80% or Higher	0+Did Not Meet/80% of lower/No
Policies & Procedures	Can the agency provide evidence of having access to an electronic or hard copy of the most recent Policies and Procedures Manual?	Yes		No – The agency did not provide evidence of access to a hard or electronic copy of the most recent P&P Manual.
Data Collection/Quality	Does the agency have a data collection protocol that is entered into HIMS in real-time (as it is collected)? If not, do the intake forms capture universal and applicable program specific data elements? (Section 6.5)	Yes		No – The agency did not provide evidence of access to a hard or electronic copy of the most recent P&P Manual.
	For data from the past 12 months, do all the agency's projects maintain data quality standards in compliance with Section 6.5?	Yes		No– The agency does not have a data collection form or protocol.
	In the past 12 months, are > 75% of the client entry and exit records being entered into HMIS within 72 hours?	Yes		No
	Do all agency programs have a 96% or higher score on the most recent data quality report?	Yes	No___/___ programs have a 96% or higher data quality score.	No
	Does the data in HMIS accurately reflect the client situation? Note: The HMIS Committee will request to review ten randomly selected records of the clients listed in the data quality report mentioned above.	Yes	No-___/___ clients have accurate information.	No-___/___ clients have accurate information.

Privacy Statement	Does the agency have the Privacy Statement posted in a common area where all clients can see it? *Appendix H	Yes		No
	Hard and/or electronic copies of the Privacy Statement are available to anyone requesting a copy.	Yes		No
	Does the agency have the most recent electronic or hard copy of the SC HMIS Statewide Privacy Policy. *Appendix D	Yes		No
	Hard and/or electronic copies of the SC HMIS Statewide Privacy Policy are available to anyone requesting a copy.	Yes		No
User Authentication	All Users abide by the HMIS policy for not sharing HMIS Usernames and Passwords.	Yes	No-___/___ Users abide by the policy.	No-___/___ Users abide by the policy.
	All agency Users have logged in to the system at least once in the past 30 days.	Yes	No-___/___ Users have logged in within the past 30 days.	No-___/___ Users have logged in within the past 30 days.
	All Users do not have their Usernames and/or Passwords displayed in a public place. (e.g., Sticky notes on monitor)	Yes	No-___/___Users do not have their Usernames and/or password in a public place.	No-___/___ Users do not have their Usernames and/or password in a public place or everyone has their credentials in a public place.
	All web browsers used to access HMIS (Wellsky Community Services) are configured to not auto-fill Usernames and Passwords	Yes		No
PII Data	Does the agency have written procedures in place to protect and store hard copy data generated from or for the HMIS?	Yes		No
	Have all Users received training on the proper storing of hard copy data?	Yes	No-___/___Users have received training.	No-___/___ Users/ no Users have received training.

	Does the agency have policies and procedures to dispose of hard copy PII?	Yes		No
	Have all Users received training on the proper disposal of hard copy data?	Yes	No-___/__ Users have received training.	No-___/__ Users have received training.
Virus Protection, Firewall, & Internet Connection	Agencies will have a person or agency in charge of IT to write a letter on agency letterhead to explain the agency's virus protection, firewall credentials, and secure internet connection.			
	Do all computers have a virus protection software package with automatic update enabled?	Yes	No-___/__ computers have virus protection with automatic update.	No-___/__ computers have virus protection with automatic update.
	Does the agency have a firewall on the PC, network and/or workstation(s) to protect the devices that are used to access the HMIS?	Yes	No-___/__ computers have a firewall enabled	No-___/__ computers have a firewall enabled
	Does the agency have a password-required secure internet connection?	Yes		No
Remote Access	Does the agency follows the Remote Access Policy included in the SC HMIS P&P Manual? (Appendix K)	Yes		No
Law Enforcement	Have all Users been trained on the procedures to follow if they are approached by law enforcement requesting data from the HMIS?	Yes	No-___/__ Users have received training.	No-___/__ Users have received training.

Physical Access	All workstations are password protected and set to auto-lock their screens after 10 minutes of inactivity	Yes	No-___/___ workstations are password protected with auto-lock enabled	No-___/___ workstations are password protected with auto-lock enabled
	All printers are accessed with access codes or printers are in a secure location where there is no public access.	Yes	No-___/___printers follow the stipulations.	No-___/___ printers follow the stipulations.
Accommodations	All Users have been trained on how to assist clients who are not English proficient or have a disability.	Yes	No-___/___ Users have received training.	No-___/___ Users have received training.
Trainings	All Users have completed the necessary HMIS trainings over the past 12 months, as outlined by the CoC.	Yes	No-___/___Users have completed all the necessary trainings.	No-___/___Users have completed all the necessary trainings.
Score	Total: /54	• 43+ points= Passed/no additional monitoring is needed for the year. • >43 points= Failed/Additional monitoring for the year is needed.		
Notes				
Administration	Additional Monitoring Needed?	Yes	No	
	Monitor Signature			
	Agency Staff Signature			