SC-211

South Carolina 211 HMIS

Homeless Management Information System

Policies and Procedures

Latest Update: May 9, 2019

Table of Contents

1 Organizational Structure 4
2 SC 211/HMIS Steering Committee 4
3 HMIS Committee 5
4 Contributory HMIS Organization 5
4.1. Agreements to Participate 5
4.2. Terms of Participation 6
4.3. Contributory HMIS Organization (CHO) 6
5 Access to HMIS 6
6 Types of Users (User ID Privileges) 7
7 Data 8
7.1. Ownership of Data 8
7.2. Data Privacy 8
7.2.1. Privacy Notice (Statement) 8
7.2.2. Privacy Policy 9
7.2.3. Acknowledgement of Receipt of Notice of HMIS Privacy Practices and Release of Information 9
7.2.4. Protected Personal Information (PPI) 10
7.3. Data Quality 10
7.4. Merging Duplicate Client Records 11
7.5. Other Data 11
7.6. Data Integrity and Accuracy 12
7.6.1. Data Timeliness 12
7.7. Information Regarding Children 12
8 Privacy and Security Plan 13
8.1. Desktop Security 13
8.2. Data Security 14
8.3. Client Data Sharing 14
8.4. Sharing Client Profile (Name, Age, SSN, Race and Gender) 15
8.5. Changing Client Demographic Information 16
8.6. Sharing Assessments and Other Data 16
8.7. Aggregate Data Sharing and Release 16
8.8. Data Extracts 17
9 Technical Support and System Availability 18
10 Appendices 18
APPENDIX A: DEFINITION OF TERMS 20
APPENDIX B: CONFIDENTIALITY GUIDELINES 22
APPENDIX C: REQUEST FOR USER ACCOUNT 23

APPENDIX D: ACKNOWLEDGEMENT OF RECEIPT OF NOTICE OF (HMIS) PRIVACY PRACTICES AND RELEASE OF INFORMATION 25
APPENDIX E: HMIS PRIVACY POLICY 26
APPENDIX F: PRIVACY STATEMENT 30
APPENDIX G: CODE OF ETHICS 31
APPENDIX H: COMPLETE HMIS INTAKE FORM 1
APPENDIX I: RESERVED 4
APPENDIX J: HMIS DATA QUALITY PLAN 5
APPENDIX K: HMIS MONITORING CHECKLIST 6
APPENDIX M: FORM ACKNOWLEDGEMENT 12

SOUTH CAROLINA 211 HMIS
HOMELESS MANAGEMENT INFORMATION SYSTEM
POLICIES AND PROCEDURES

This document defines the Policies and Procedures of the SC-211 Homeless Management Information System (HMIS). SC-211 HMIS encompasses the four Continua of Care in South Carolina: Eastern Carolina Homelessness Organization (ECHO), Midlands Area Consortium for the Homeless (MACH), Upstate Continuum of Care (UCoC), Lowcountry Homeless Coalition (LHC), 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. **CoC Programs may not deny services or housing to clients for failure to participate in the HMIS.**

Capitalized terms are defined in Appendix A.

1 Organizational Structure

Policy: HMIS shall be governed by the primary decision making body of the Continuum of Care (CoC) of the community plan. 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 system. 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 MOAs 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 the HMIS Data and Technical Standards.

Procedure: The CoC's HMIS Lead Agency shall be responsible for selecting and designating the representative to the SC-211 Steering Committee.

2 SC 211/HMIS Steering Committee

Policy: Primary decisions regarding SC-211 that affect all **lead agencies (i.e. CoC, HMIS HMIS Lead Agency)** are made by the SC 211/HMIS Steering Committee. The HMIS/211 Sharing Agreement defines the Steering Committee and its responsibilities.

Procedure:

1. As defined in the **CHO** HMIS sharing contracts, the Steering Committee is comprised of at least one person designated by each **HMIS Lead Agency and 211 Parties**. It shall meet, as needed, to make decisions regarding:
   - Implementation / Training
   - Expansion
   - Project management
   - Oversight
   - Enforcement
   - Coordination
   - Contracts

- Policies and Procedures

2. Meetings shall be called by the SC 211/HMIS Steering 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 are in agreement.

3 HMIS Committee

Oversight Committee of CoC's HMIS

Policy: Each CoC shall designate a local committee ("HMIS Committee") to oversee the implementation of the HMIS and establish policies governing the HMIS. Policies must adhere to the guidelines set forth in the HUD HMIS Data and Technical Standards. This committee makes 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 HMIS Committee and that its responsibilities are tracked and documented.

4 Contributory HMIS Organization

4.1. Agreements to Participate

Policy: All CHO in the HMIS must have a signed agreement with the HMIS Lead Agency. The HMIS Lead Agency must execute a Memorandum of Agreement, Memorandum of Understanding or some form of an agreement with each Contributory HMIS Organization (CHO) (an "Agreement to Participate"). The agreements must reference these 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 agreements must define the terms of participation for all parties as well as the obligations and authority of the HMIS Lead Agency.

Procedure: Any Agreement to Participate 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.

4.2. Terms of Participation

Policy: All Agreements to Participate will include the following 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 shall be outlined in the MOA among all CHO.

4.3. Contributory HMIS Organization (CHO)

Policy: Participation will be limited to 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, (2) permanent supportive housing, (3) service agencies targeting the homeless population, and (4) other agencies serving at-risk populations. Domestic Violence shelters are prohibited by HUD from participating in HMIS.

Procedure: All parties seeking to participate must contact the HMIS Lead Agency and provide information on the CHO and demonstrate ability to comply with the SC-211 Policies and Procedures.

5 Access to HMIS

Policy:

1. Access to the HMIS is restricted to only those with a valid User ID and password. Only a CHO that has signed the Agreement to Participant 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.
2. **User IDs may not be shared**. It 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 Agreement to Participate with **the HMIS Lead Agency**. 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 coalition or **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, a fee per license may be assessed based on availability or limited resources.
4. All new Users must complete training prior to access, which consists of four components:
    - ServicePoint Application
    - Data Quality

- Security
- Privacy

5. Prior to training, each User must sign and initial the **Request for HMIS User ID** form. The form must also be signed by the User's immediate supervisor and the CHO's Executive Director. Training may be provided by the HMIS CoC Administrator or other persons or organizations authorized by the HMIS 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 form must be signed by the CHO, Executive Director of the subcontractor CHO, and system User.
7. Each User must complete the HMIS Privacy Questionnaire.
8. Each User must read the HMIS Privacy Policy and the HMIS Code of Ethics prior to accessing the HMIS for the first time and to the extent reasonable, each User must sign an acknowledgement of having done so.
9. **The CHO is responsible for informing its regional HMIS CoC 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.**
10. 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 will be known only by the User and may not be shared.

    Users are required to follow the Policies and Procedures defined in this document, which 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 at: http://schomeless.org.

    Failure to comply with these Policies plus and HMIS Lead Agency policies may result in the suspension or revocation of a User ID.

6 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.

Case Managers who enter data for more than one CHO must sign a Business Associates Agreement (BAA) with their **CHO,** as these Users will have access to data from multiple CHO. Copies of the signed BAA should be provided to the HMIS CoC Administrator.

3. **"CHO 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 reassign temporary passwords for Users in their agency. CHO 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 System Administrator) may request a CHO 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 System Administrator II of the HMIS Lead Agency to request training for potential new HMIS Users and will specify the requested privileges of such potential User. Once trained, a User ID and temporary password are created and provided in accordance with Section 5 above. The CHO Administrator or HMIS CoC Administrator will ensure that training is consistent with the User level and need.

7 Data

7.1. 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 7.2.3 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 Memorandum of Agreement as set forth in Appendix and as elsewhere stated in this document, or with the SC Revenue and Fiscal Affairs Office (RFA) for research purposes with identifiers, provided there is a signed MOA among the CoC, the HMIS Lead Agency, and RFA stating client identifiers will not be released to any third party, are destroyed after a specified period of time and otherwise meet requirements of these Policies and Procedures document and relevant law.

Procedure: Data is stored on a server in a secure location at WellSky.

7.2. Data Privacy

7.2.1. Privacy Notice (Statement)

Policy: Each CHO must post a copy of the Privacy Statement at each intake desk (or comparable location) and on the CHO's web page that explains the reasons for collecting data and the general use and disclosure of such information.

Procedure: A CHO may modify this statement or combine it with existing privacy statements; provided, however, that any modifications must be approved by the HMIS Lead Agency and comply with applicable law.

7.2.2. Privacy Policy

Policy: Each CHO will abide by the HMIS **Privacy Policy,** which defines the privacy practices of all CHO.

Procedure: Each CHO must have a copy of the HMIS **Privacy Policy** (included in Appendix E). The HMIS Privacy Policy must be provided to clients. If a client is illiterate, the CHO must assure 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, and limited English proficiency.

7.2.3. Acknowledgement of Receipt of Notice of HMIS Privacy Practices and Release of Information

Policy: Clients have an ownership interest in the data they provide, subject to certain limitations under applicable law. Absent consent by a client, no client data may be shared with another HMIS CHO. A CHO may assume an implied consent provided that the individual has a reasonable opportunity to object and no disability information (HIV/AIDS, substance abuse, mental illness, or other disability whose release is covered by state or federal release regulation) is shared.

Procedure: Data collected is essential to the administration of local assistance programs. We recommend that each CHO has its clients sign the *South Carolina 211 Homeless Management Information System (HMIS) Release of Information Form ("ROI").* This form has a place for the client to sign indicating they have read and understand what data is collected and how it might be used. The *Release of Information* has a separate section where the type of information released is identified and a separate signature block is available. Clients are encouraged to sign this section. *The Alternate Notice of Privacy and Release of Information* are used when a signature is not obtained, but a staff member certifies that the client was given the notice. The *Acknowledgement of Receipt of Notice of HMIS Privacy Practices and Release of Information* form is provided in Appendix D.

This sharing practice is useful in creating unduplicated client counts and to facilitate effective client case management. All clients should be encouraged to sign the Acknowledgement and Release. Data is only shared with another CHO that has access to HMIS or as specified elsewhere in this document.

The default setup is ALWAYS to share data with all other CHO with client's consent. The release of information initiates the sharing of information with other CHOs. Any CHO that has a client that does not consent to the ROI must assume the responsibility of securing the necessary client information within the HMIS profile so that any new information is not shared openly within HMIS.

The ROI expires after one year and should be updated each year when the client's assessment is completed.

Assuming the prior Release of Information (ROI) has not been revoked, after the release of information expires, the information remains in the system, but any new information added is not shared. It is the responsibility of the CHO to secure any new client information within HMIS.

Any changes to the Privacy Policy and Acknowledgement of Receipt of Notice of HMIS Privacy Practices must be approved by the HMIS Lead Agency.

7.2.4. Protected Personal Information (PPI)

Policy: Information that uniquely identifies an individual is Protected Personal Information (PPI) and such information will be protected against improper use and disclosure in accordance with applicable state and federal regulations. The Client Profile (Name, Date-of-Birth, Social Security Number, Race and Ethnicity) are the key primary identifiers we collect and are examples of PPI.

Procedure: All clients must be informed, via a posted **Privacy Statement** and/or the **Acknowledgement of Receipt of Notice of HMIS Privacy Practices and Release of Information** form, that we do not release this or any other information to other Users on the system or anyone else without their express or implied consent. In the event a client wants to stop the sharing of his/her information before the expiration of their Release of Information, the request must be made in writing and a copy will be sent to the HMIS Lead Agency. Note that psychotherapy notes and records relating to behavioral health and substance abuse are subject to heightened rules regarding their use and disclosure. Each CHO is responsible to assure that only legally-permitted information is provided under applicable law including, without limitation, under HIPAA and "Part 2" (42 CFR Part 2) limitations on disclosure of substance use disorder patient records.

7.3. Data Quality

Policy: The HUD HMIS 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.

7.4. Merging Duplicate Client Records

Policy: In order to avoid duplicate client records, Users should always search for an existing client record before creating a new client. In the event that an End User finds duplicate records for a client, the End User should submit an email request to the HMIS Lead Agency.

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 (for example, a point-in-time count survey), in which case the system administrator should use his or her discretion.

Locked records subject to unique security regulations (i.e. HIPAA, RHYMIS) 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.

7.5. 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 a large number of 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. Some of the possible assessment screens include:

- Children
- Children Immunizations
- Client Budget and Expenses
- Education
- Employment
- Insurance
- Legal
- Medical
- Mental Health
- Person Strengths
- Psychosocial
- Addiction
- Family / Residence
- PAT (PATH grants ONLY)
- Coordinated Entry Assessments

7.6. Data Integrity and 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. Data may be entered, and corrected if necessary, within 72 hours of when the data is provided by the client.

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

To improve data quality, the HMIS CoC Administrator shall run data reports which show clients with missing Universal Data Elements and clients with missing Program Data Elements, and any Users that are part of a CHO will receive a copy of the data quality reports. These reports will be emailed to all Users with data entered or updated within the last 30 days from when the report is run listing clients with missing data and the data items that are missing. Please see Section 3 of the of the HMIS Data Standards Manual for required Universal Data Elements and Section 4 and Appendix B of the of the HMIS Data Standards Manual for Program Data Elements required by HUD. Reports are to be run at at the discretion of the HMIS Lead Agency.

HUD CoC data quality benchmarks for null data are:

- Gender – 0.3%
- Ethnicity – 3.4%
- Race 7.7%
- Age 1.0%
- Veterans Status – 7.5%
- Disability Status – 22.0%
- Living Arrangement Prior to Program Entry – 21.3%
- Length of Stay - 28.9%
- ZIP Code of last permanent Address – 27.1%
- Overall data completeness – 96%

7.6.1. Data Timeliness

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.

Policy: Users must make their best efforts to enter data collected from client interviews within 72 hours.

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.

7.7. Information Regarding Children

Whenever possible, the CHO should not receive information directly from a child under the age of 13 without the parent's express written consent. 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) obtain verifiable (written) parental consent; (3) provide, upon the parent's request, 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 SC-211 protecting the confidentiality, security, and integrity of information will apply to all personal information of children.

8 Privacy and Security Plan

The privacy of client data is to be of the utmost concern for all Participants and Users.

8.1. Device Security

Policy: ServicePoint, the software used for the HMIS, is accessed via the Internet. A broadband Internet connection is necessary. To maintain security, devices 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.

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

A recent release of a browser that supports 256 bit TLS encryption, such as Google, Chrome, Internet Explorer 11, Microsoft Edge, or Mozilla Firefox latest version.

A vendor supported and updated operating system. These include Microsoft Windows 8/8.1/10 and Mac OS X v10.11.6 or newer.

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 device 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 a subscription service to keep it up-to-date, and the subscription must be kept current.

All devices must be kept in secure locations at all times and not left unattended while unlocked.

All devices used for access to HMIS that are not in a locked room must use a screen saver set for 10 minutes or less and require a password to reactivate.

The HMIS Systems Administrator can help set up devices, if needed. Printers must have access code protection or be maintained in a locked office.

HMIS User passwords must not be written down and left near computers used to access HMIS.

8.2. 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:

- All Users are issued a *unique* User ID and temporary password to access the system in accordance with Section 5 above.
- All Users must sign confidentiality statements and attend training that includes information on data security.
- Hard copies of data must be stored in a locked file cabinet.
- HMIS 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 10 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")).
- Computers must be set to lock after 10 minutes of inactivity and must be protected with a screen saver.
- Computers are not to be left alone with PPI data displayed.
- After 3 failed log-ins, the User's password will be inactive.
- 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 PPI stored on a computer must be encrypted in accordance with the current industry standard.

8.3. Client Data Sharing

Policy:

HMIS has five types of data:

1. Client Profile. If set to share in the Provider's Profile, does not require an ROI to be entered to be shared.
2. Primary assessment data. This data is captured on the primary assessment page used by the CHO.
3. Client needs and services provided.
4. Goals and case notes.
5. Other Assessment data not included in 1. or 2. above.

We define three levels of data sharing:

1. Not shared.

2. Shared globally (all other Users on the HMIS).
3. Selective sharing (specified CHO list for each type of data defined above for each CHO).

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

- Client Profile data is shared globally and does not require an ROI to be shared.
- Primary assessment, Household Data Sharing, and Needs/Services are shared globally, but require an ROI with positive permission and an active date range to be entered before data is shared.
- All other data is closed (not shared) such as case notes, but a CHO may request any specific assessment or group of data defined in HMIS to be shared, either globally or to a specific CHO.

ALL providers for mental health services or any CHO whose primary clients are youths (defined as minor 17 years and below), or any CHO whose primary services are for HIV/AIDS or substance abuse, are set to only share Client Profile, and this may be set to not shared if requested. (Note: Client Profile data does NOT include any information about which CHO entered the data.)

Procedure: The majority of provider profiles in the HMIS are set to share globally.

Thus, all CHO must use the Privacy Policy and ROI form, which explicitly states the purposes for which the CHO collects data and provides places for signatures and date. Two of the stated purposes for collection of data are continuity of care and research.

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) will limit the use and disclosure of any protected health information to any individual or organization.

8.4. Sharing Client Profile (Name, Age, SSN, Race and Gender)

Policy: Client Profile is shared by default. This data is shared if the client has signed a ROI form indicating that the client has agreed to share this data with all HMIS CHO or the disclosure is otherwise permitted by these policies (e.g., in case of an emergency and certain disclosures where there is an implied consent).

Procedure: Provide all clients with a copy of the Privacy Policy and have all clients sign the *Acknowledgement of Receipt of Notice of HMIS Privacy Practices and Release of Information (ROI)* form (Appendix D). This should be the one provided by your HMIS Lead Agency or one that has been approved by the CoC. If the CHO is using implied consent, a CHO staff member should sign the Notice indicating the client has been informed of the Privacy Policy and consents. If the CHO is sharing information with a third party, the client must complete and sign the consent form in Appendix L.

8.5. Changing Client Demographic Information

Policy: If a User observes incorrect demographic information in a client profile that he or she did not create, the User should send an encrypted email to the HMIS Lead Agency or the User can make changes based on verified documentation.

Procedure: The HMIS Lead Agency should correct the client demographic information after verifying that the User requesting the change has documentation of the correct information (i.e. driver's license or social security card). Staff observations should NOT be used to collect information on clients' ethnicity. All clients must be asked to self-report any ethnicity information, and no documentation is required to verify a client's response.

8.6. Sharing Assessments and Other Data

Policy: A CHO may share additional client data with another HMIS CHO for the purposes of facilitating a referral for services or housing only if the client has signed a ROI or otherwise consented and a release of information with permission to share has been entered by the **User in the system.** Clients may not be denied housing or services based on a failure to sign a ROI. A CHO may use an implied consent if desired, except as otherwise noted in this document, but CHO staff should sign the *Notice* indicating the client has been informed and consents.

Procedure: To share assessment data:

1. Have the client sign the ROI . This includes consent to enter data into the system and consent to share additional information. Two (2) signatures are required. The *Release* document may also be used for implied consent and only the CHO staff needs to sign.
2. There are certain CHO that share data only in HUD verification section and do not share clinical data globally. These include CHO whose primary function is to serve those with mental health conditions and HIV/AIDS.

8.7. Aggregate Data Sharing and Release

Reports:

Policy: Reports generated by any CHO or the HMIS Lead Agency may be made public and/or shared with another CHO and organizations PROVIDED the report contains NO CLIENT IDENTIFIERS. Client level data will be used by the HMIS Grantee/CoC for research, CoC planning purpose, and HUD required Coordinated Entry System Purposes.

Procedure: Any reports that include any of the following information, or regarding which you know the information could be used to identify an individual, MAY NOT BE shared outside of HMIS or your agency with the exception of RFA or as required by the Coordinated Entry System as elsewhere noted in this document. The following are considered "identifiers":

1. Names;
2. 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.

3. 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;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

8.8. 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.

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 Data Use Agreement ("DUA") in place between the CoC and HMIS Lead Agency and the third party. The DUA must include a provision that restricts use of client identifiers to 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. However, the data with client identifiers cannot be reproduced in any form, and it must be deleted once its purpose of data matching is complete. The CoC and HMIS Lead Agency must review research findings and authorize release of findings based on HMIS data. Additionally, extracts may be shared for the purposes of compliance with HUD's required Coordinated Entry System.

Procedure: To share data with a third party for the purpose of research and aggregate reports with data matched from other data sources, the **CHO** must have a signed DUA(or contract) with the third party explicitly detailing the constraints of access to, reproduction of, and distribution of the data as outlined above. The DUA must be reviewed by the HMIS Lead Agency prior to signing. As named on the consent form, the entity that discloses information must, within 30 days of a client's written request, provide to the client: (1) the name of the entity to which the disclosure was made; (2) the date of the disclosure; and (3) a brief description of the identifying information disclosed.

9 Technical Support and System Availability

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

Procedure: Users should call or send an email to the HMIS Lead Agency or the designated technical assistance contact for the CoC.

In addition, a 'HMIS Monitoring Checklist' of HMIS Requirements, Response (compliance), Assessment and Action Items is included in the Appendix. This document should be used by the CHO to ensure compliance with the Policies and Procedures. The CoC designated HMIS person may periodically review CHO and User compliance with Policies and Procedures and assist, where practical, with technical support to help such CHO comply.

10 Appendices

Included in the Appendices are copies of a number of forms used by each coalition. Those included in these Appendices are representative examples of those forms, which may be different for each coalition. Electronic copies of the latest version of your coalition's current forms are available online – contact your HMIS CoC Administrator for access and are sure that you are using the most recent forms, as these may change from time to time.

Appendix A:	**Definition of Terms**
Appendix B:	**Confidentiality Guidelines**
Appendix C:	**Request for User Account**
Appendix D:	**Acknowledgement of Receipt of Notice of (HMIS) Privacy Practices and Release of Information**
Appendix E:	**Privacy Policy**
Appendix F:	**Privacy Statement**
Appendix G:	**HMIS Code of Ethics**
Appendix H:	**Complete HMIS Intake Form**
Appendix I:	**Reserved**
Appendix J:	**Data Quality Plan**
Appendix K:	**Agency/Site Data Standards Compliance Checklist**
Appendix L:	**Memorandum of Agreement**

Appendix M: Form Acknowledgement

Please contact your HMIS Lead Agency for electronic versions of these documents.

APPENDIX A: DEFINITION OF TERMS

1. "Business Associate Agreement" or "BAA" – An agreement signed between a "covered entity" under HIPAA (i.e., a health care provider, payor or clearinghouse) and a subcontractor (a "business associate") with access to PPI, or between a business associate and a further downstream contractor.

2. "Client Profile" – Primary client identifiers in the HMIS: name, date-of-birth, social security number, race, gender, and veteran status.

3. "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.

4. "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 Protected Information (PPI) to the system.

5. "Data Use Agreement" or "DUA" in place between the CoC and HMIS Lead Agency and the third party. The DUA must include a provision that restricts use of client identifiers to 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. However, the data with client identifiers cannot be reproduced in any form,

6. "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.

7. "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 and who qualifies for access to the HMIS in accordance with these Policies and Procedures.

8. "HMIS CoC Administrator" – The HMIS-appointed administrator, 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 HMIS CoC Administrator.

9. "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.

10. "Homeless Management Information System" or "HMIS" - The information system designated by a CoC to process Protected Personal Information (PPI) 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.

11. "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*.

12. "MOA" – A Memorandum of Agreement (MOA), which must be executed between the Grantee and all participating agencies. The documents must be signed by the Executive Director of the CHO.

13. "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.

14. "Privacy Policy and Acknowledgement of Receipt of Notice of (HMIS) Privacy Practices and Release of Information" or "ROI" – A document detailing the HMIS Privacy Policy similar to a standard HIPAA Notice of Privacy Practices. The document addresses the client's confidentiality rights; information rights; information security; benefits of agency information sharing; risk in sharing information and questions; and risks a client should consider. The ROI includes a standard Acknowledgement of Receipt of Notice of (HMIS) Privacy Practices form, a place to sign indicating the client has been informed of the agency's policy and a place to sign the consent to release information with all CHO. For CHOs that are "covered entities" under HIPAA, the ROI will *not* serve as a Notice of Privacy Practices.

15. "Protected Personal Information" or "PPI" – 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 reasonable 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 PPI. PPI 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.

16. "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.

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

18. "ServicePoint" – The HMIS application used by HMIS. It is licensed from WellSky.

19. "South Carolina Coordinated Entry System HMIS Code of Ethics" – A set of guiding principles for the CHO and Users of the HMIS**.**

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

APPENDIX B: 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-211 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-211 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.

1. 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.

2. 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.**

3. The CHO will make a copy of the SC-211 HMIS Privacy Statement available to any client requesting a copy.

4. 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.

5. 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.

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

7. 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.

APPENDIX C: REQUEST FOR USER ACCOUNT

SOUTH CAROLINA COORDINATED ENTRY SYSTEM
REQUEST FOR HMIS (ServicePoint) USER ACCOUNT

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

Contact your local CoC Administrator

Please complete the following:

Agency Name: _____

Employee Name & Position Title: _____

Employee Email Address: _____

Employee Contact Number: _____

USERS RESPONSIBILITIES/PROCEDURES

- Except in job-sharing situations, each user requires a unique username and private password. 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 will be assigned and emailed to the user. Upon receipt, the user should call the HMIS CoC Administrator for their temporary password.
- All End Users must obtain and review a copy of the HMIS Policies and Procedure, which includes Privacy Statement, Security, and Data Quality sections.
- After reviewing the Confidentiality Guidelines **(Appendix B)** please sign the Confidentiality and Responsibility Certification **(next page).**

HMIS USER
CONFIDENTIALITY AND RESPONSIBILITY CERTIFICATION

I have read the Confidentiality Guidelines and I agree to maintain strict confidentiality of information obtained through the SC-211 Homeless Management Information System (HMIS). This information will be used only for legitimate client service and administration of the agency listed below. Any breach of confidentiality will result in immediate termination of participation in 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 properly destroyed to maintain confidentiality.

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

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

____ I will notify the appropriate parties within 24 hours of termination of employment.

____ I have completed the HMIS Privacy Questionnaire.

____ 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.

Employee's Signature_____ Date: _____

Supervisor's Signature _____ Date: _____

Executive Director's Signature: _____ Date: _____

System Administrator Signature: _____ Date: _____

APPENDIX D: ACKNOWLEDGEMENT OF RECEIPT OF NOTICE OF (HMIS) PRIVACY PRACTICES AND RELEASE OF INFORMATION

ACKNOWLEDGEMENT OF RECEIPT OF NOTICE OF SC-211 HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS) PRIVACY PRACTICES AND RELEASE OF INFORMATION

Notice of Privacy

I, (Client Name) _____ , have received the Notice
Print Client Name

of Privacy Practices from an HMIS participating agency.

X _____ Date: _____
Client/Parent/Guardian Signature

Relationship if parent/guardian: _____

Release of Information

Type of information to be released may include:

- **Profile and Assessments**
- **Financial/Work-History/Residential Information**
- **Mental Health Assessment/Progress**
- **Substance Abuse Assessment/Progress**
- **Medical / Health Information**
- **Needs and Services Provided**

This information is to be released for the purpose of continuity of care/case management and or client advocacy and is valid for one year unless otherwise specified.

X _____ Date: _____
Client/Parent/Guardian Signature

Relationship if parent/guardian: _____

Alternate Notice of Privacy and Release of Information (not to be used if client information to share includes: alcohol or drug abuse, HIV/AIDS, or mental health diagnosis or treatment)

*In lieu of client signature, I _____ , a staff member of an HMIS
Print Staff Name

participating agency, state that _____ , has been given our current Notice of Privacy Practices.
Print Client Name

_____ Date: _____
Staff Signature

APPENDIX E: HMIS PRIVACY POLICY

This Privacy Policy guides the operation of HMIS and all of its users. All users should be familiar with this policy and must be provided a copy prior to receiving a user ID and access to HMIS. The Privacy Statement (APPENDIX E) is to be posted at intake/assessment stations where clients can see it, must be described to each new client, and a copy must be offered to each new client.

The HMIS was developed to meet a data collection requirement made by the United States Congress to the Department of Housing and Urban Development (HUD). Congress passed this requirement to obtain a more accurate count of individuals who are homeless and to identify the need for and use of different services by those individuals and families. To provide documentation toward improving homelessness, Congress implemented the collection of statistical information on clients who access services documenting that information in a central data collection system.

Partner agencies in the state of South Carolina also use the HMIS to keep computerized case records. With the client's permission, most agencies share information with other agencies on the HMIS. The information that you agree to allow HMIS to collect and share includes demographic and assessment information and services provided. Sharing information with the HMIS and other agencies helps to better understand the number of individuals who need services from more than one agency. This assists us in meeting your needs and the needs of others in the community by allowing HMIS and its partner agencies to develop new and/or more efficient programs. Sharing information through HMIS also helps making referrals easier, often with less paperwork for you.

Maintaining the privacy and safety of those using the services of HMIS and its partner agencies is very important. Information gathered about you is personal and private. **We collect information only when appropriate to provide services, to manage our organization, for research, or as required by law.** Your record will be shared only if you give your permission. Depending on your individual situation, there may be benefits and/or risks which you should consider carefully before you decide whether or not to consent to release of any identifying information to another agency. You cannot and will not be denied services that you would otherwise qualify for if you choose not to share information.

Please note, even if you do not want your information shared with other agencies or your actual name entered into the system, we must still report some information to the central data collection system. This system contains provisions to protect your name and privacy.

CONFIDENTIALITY RIGHTS

The partner agency has a confidentiality policy that has been approved by its Board of Director. The policy follows all HUD and HIPAA confidentiality regulations that are applicable to the agency, including those covering programs that receive HUD funding for homeless services (HMIS Data Standards (August, 2014)). The HIPAA privacy and security rules and Part 2 Rules govern confidential health information, such as the diagnosis or treatment of a mental health disorder, a drug or alcohol disorder and AIDS/HIV condition or domestic violence situation. Even if you choose to allow us to share information with other agencies, records about substance abuse, physical and mental health, HIV, and domestic violence will **not** be shared without your specific written release of information.

This agency is restricted to using or disclosing personal information from the HMIS only in the following circumstances:

- To provide or coordinate services to an individual.
- For functions related to payment or reimbursement for services.

- To carry out administrative functions including, but not limited to, legal, audit, personnel, planning, oversight and management functions.
- Contractual research where privacy conditions are met and prior written approval has been obtained from the HMIS Grantee and CoC. Research findings must be reviewed by the HMIS Grantee and CoC and written approval granted prior to release of findings.
- Where a disclosure is required by law and disclosure complies with and is limited to the requirements of the law. Instances in which this might occur are during a medical emergency, to report a crime against agency staff, or to avert a serious threat to health or safety

INFORMATION RIGHTS

As a client receiving services at this agency, you have the following rights:

- Access to your record. You have the right to review your HMIS record. At your request, we will assist you in viewing the record within 7 working days.

  An agency may deny you the right to inspect or copy your personal information for the following reasons: (1) information is compiled in reasonable anticipation of litigation or comparable proceedings: (2) information about an individual other than the agency staff would be disclosed; (3) information was obtained under a promise of confidentiality other than a promise from this provider and disclosure would reveal the source of the information; or (4) disclosure of information would be reasonably likely to endanger the life or physical safely of an individual.
- Corrections to your record. You have the right to request to have your record corrected so that information is current and accurate to ensure accuracy. You have 45 days from the date the information is entered to request a correction.
- Refusal. You have the right to refuse consent to share your information with other agencies. You cannot be denied services that you would otherwise qualify for if you refuse to share information. Please note that if you refuse this permission, information will still be entered into the system for statistical purposes.
- End of Consent and Withdrawal of the Release of Information. You have the right to change your mind about consent or release of information that you have already granted. You have 45 days from the date you signed the consent or release to revoke it.
- Harassment. The agency reserves the right to reject repeated or harassing requests for access or correction. However, if the agency denies your request for access or correction, you will be provided written documentation regarding your request and the reason for denial. A copy of that documentation will also be included in your client record.
- Grievance. You have the right to be heard if you feel that your confidentiality rights have been violated, if you have been denied access to your personal records, or you have been harmed or put at personal risk. Send a written statement to the local Continuum of Care lead agency within 7 business days of an incident.
- Note: HMIS is not used to share any personally identifiable information collected with law enforcement agencies, except by court order or subpoena.

INFORMATION SECURITY

Protecting the safety and privacy of individuals receiving services and the confidentiality of their records is of paramount importance to us. Through training, policies and procedures, and software we have taken many steps to ensure your information is kept secure.

- The computer program we use includes security protection software and hardware.

- Only trained and authorized individuals will enter or view your personal information.
- Your name and other identifying information will not be contained in local reports.
- Employees receive training in privacy protection and agree to follow strict confidentially guidelines.
- The server/database/software is designed to allow only authorized individuals to access the information.
- The server/database will communicate using encryption – an Internet technology intended to keep information private while transporting data. Furthermore, identifying data stored on the server is also encrypted or coded.
- The System Administrator(s) supports the daily operation of the database. Administration of the database is governed by agreements that limit the use of personal information to providing administrative support and generating reports.

BENEFITS OF AGENCY INFORMATION SHARING

Information you provide us is important to the ability of all agencies to continue to provide the services that you and others in our community are requesting.

Allowing us to share your real information results in a more accurate count of individuals and services used and helps us to:

- Better demonstrate the need for services and the specific types of assistance needed in our area
- Obtain more funds and other resources to provide services
- Plan and deliver quality services to you and your family
- Assist the agency to improve its work with families and individuals who are homeless
- Keep required statistics for state and federal funders.

You may choose to share additional information with other agencies in order to:

- Promote coordination of services so your needs are better met.
- Make referrals easier by reducing paperwork.
- Avoid having to repeat information to get assistance from other agencies using the CAS.

RISKS IN SHARING INFORMATION

While this system is secure and promotes better service delivery to the homeless or those at-risk of becoming homeless, there are risks that may lead clients to choose to do the following:

- Allow only your name, age, date of birth, social security, and services to be shared with other agencies. All other information will be kept confidential.
- Allow some statistical or demographic information to be shared to include assessment information.
- Allow demographic information and services, but not assessment information to include mental health, drug/alcohol use/history and domestic violence information.
- Close all information so that only the System Administrator(s) can see the information.

QUESTIONS AND RISKS YOU SHOULD CONSIDER

- Could there be physical harm or other negative consequences to your or members of your family if someone knew that they could find you from the information shared with other participating agencies?

- Could there be physical harm or other negative consequences to you or members of your family if someone found out you were provided with help, especially if you or your child has experienced domestic violence, sexual assault, stalking, or child abuse?

Privacy Notice Amendments: The policies covered under this Privacy Notice may be amended over time and those amendments may affect information obtained by the agency before the date of the change. All amendments to the Privacy Notice must be consistent with the requirements of the Federal Standards that protect privacy of consumers and guide the implementation and operation of the related policies.

APPENDIX F: PRIVACY STATEMENT

Please read the following statements (or ask to have someone it read to you), and make sure you have had an opportunity to have your questions answered.

_____is a participant in the SC-211 Homeless Management Information System or "HMIS" which is used by provider agencies to record information about clients they serve. This information helps the agencies to plan for and provide services to clients. It also allows for the sharing of information among agencies to improve coordination and delivery of services to you. We wish to notify you of the following information regarding data collection and storage in a client information system.

We collect personal information directly from you to coordinate services and continuity of care. We may be required to collect some personal information by law or by organizations that provide funds to operate this program. Other personal information we collect is important to operate our programs, to improve services to you, and to better understand the needs of persons experiencing homelessness. We only collect information considered to be appropriate.

Only summary information **without** your name or other personal identifiers will be reported to offices and organizations that plan and fund homeless services. We do not share any personally identifiable information collected with law enforcement agencies or any other organizations outside of HMIS without your written consent, except as provided herein or by court order or subpoena. **You cannot be denied housing or services for failure to provide written consent to share your information.**

Any information about the **diagnosis or treatment of a mental health, drug or alcohol disorder, HIV/AIDS, or domestic violence will not be disclosed without your written, informed consent.**

Besides coordinating services and continuity of care, information collected about you may be used and disclosed to:

- Improve the quality and care of services provided.
- Administer programs.
- Comply with legal requirements.
- Protect victims of abuse and neglect.
- Participate in research.
- Avert serious threat to health/safety.

We will take reasonable precautions to protect personal information in the system from unauthorized modification, use, and disclosure.

APPENDIX G: CODE OF ETHICS

As an employee or Volunteer of a participating member/CHO of the SC-211 Homeless Management Information System (HMIS) I will:

Agree to abide by all policies and procedures of the HMIS.

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 Homeless Management Information System (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 of 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 into the HMIS in settings outside of the agency.

HMIS Grantees 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. Upon receipt of satisfactory assurances that such violations did not occur or that such violations have been fully corrected or eliminated, HMIS Grantees in their discretion may resume usage.

APPENDIX H: COMPLETE HMIS INTAKE FORM

Client Name (First and Last): _____ Alias: _____

Contact Information:

Phone: _____ Accept texts? Y / N Email: _____

Emergency Contact: _____ Relationship to Client: _____

Phone number: _____ Email: _____

Client Information:

Date of Birth: _____/_____/_____ Social Security Number: _____- _____-_____

Race**:** (*Write in box a **1** for primary, **2** for secondary*)
☐ Black ☐ White ☐ American Indian/Alaskan ☐ Asian ☐ Hawaiian/Pacific Islander

Ethnicity: ☐ Hispanic ☐ Non-Hispanic

Gender: ☐ Male ☐ Female ☐ Transgender *M to F* ☐ Transgender *F to M* ☐ Gender non-conforming

Disabling Condition: ☐ Yes ☐ No ☐ Unsure ☐ Refused U.S. Veteran: ☐ Yes ☐ No

Residence Prior to Entry: (check 1)

Homeless
- ☐ Place not meant for human habitation (no electrcity or running water)
- ☐ Emergency shelter ☐ Safe Haven (Only located in Greenville) ☐ Interim housing
- ☐ Foster care ☐ Hospital or other residential non-psychiatric medical facility

Institutional
- ☐ Jail, prison, or juvenile dentention center ☐ Long-term care facility or nursing home
- ☐ Psychiatric hosptial/facility ☐ Substance abuse treatment facility or detox center

Transitional/Permanent
- ☐ Hotel paid for without emergency shelter voucher
- ☐ Owned by client, no ongoing housing sudsidy ☐ Owned by client, with ongoing housing subsidy
- ☐ Permanent housing for formerly homeless persons (e.g., CoC progeject, HUD legacy programs)
- ☐ Rental by client, no ongoing housing subsidy ☐ Rental by client, with VASH housing subsidy
- ☐ Rental by client, with GDP TIP subsidy ☐ Rental by client, with other ongoing housing subsidy
- ☐ Residential project or halfway house with no homless criteria
- ☐ Staying/living with a family member's room, apartment, or house
- ☐ Staying/living with a friend's room, apartment, or house ☐ Transitional housing for homeless

Approxiamtely…

Length of stay in previous place: _____ Date homelessness began: _____

HMIS Intake Form HMIS #: _____ Date: ___/___/____ 2

Number of **times** homelessness has occurred in the past *three* (3) *years*: _____

Number of **months** homlessness has occurred in the past *three* (3) *years*: _____

Monthly Cash Income

- ☐ Earned Income: $ _____
- ☐ Unemployment Insurance: $ _____
- ☐ Supplemental Security Income: $ _____
- ☐ Social Security Disability Income: $ _____
- ☐ VA Service Disability Compensation: $ _____
- ☐ VA Non-Service Connected Disability: $ _____
- ☐ Private Disability Insurance: $ _____
- ☐ Workers Compensation: $ _____
- ☐ TANF: $ _____
- ☐ General Assistance: $ _____
- ☐ Retirement Income from SS: $ _____
- ☐ Pension/Retirement: $ _____
- ☐ Child Support: $ _____
- ☐ Alimony: $ _____
- ☐ Other Source: $ _____

Monthly Non-Cash Income

- ☐ SNAP (Food Stamps): $ _____
- ☐ Supplemental Nutrition (WIC) $ _____
- ☐ TANF Child Care Services: $_____
- ☐ TANF Transportation Services: $ _____
- ☐ Other TANF-funded Services: $ _____
- ☐ Public Housing (Section 8, etc): $_____
- ☐ Temporary Rental Assistance: $ _____
- ☐ Other Source: $_____

Does the client have **health insurance**? ☐ Yes ☐ No If **yes**, check all that apply:

☐ Private Pay ☐ Medicaid ☐ Medicare ☐ VA Medical Services ☐ Employer provided

☐ State Insurance for Children (S-CHIP) ☐ State Insurance for Adults ☐ COBRA

☐ Indian Health Service (HIS)

Disabilities

Does the client have any of the following conditions? If **yes**, check the first box. ☒ / ☐

If the condition impairs the clients ability to **live indepently**, check the second box. ☒ / ☒

☐ / ☐ Alcohol Abuse ☐ / ☐ Drug Abuse ☐ / ☐ HIV/AIDS ☐/☐ Chronic Health Condition

☐ / ☐ Mental Health Conidtion ☐ / ☐ Physical Disability ☐/☐ Developmental Disability

HMIS Intake Form HMIS #: _____ Date: ___/___/____ 3

Domestic Violence

Has the client **ever** experienced domestic violence? Yes ☐ No ☐

How long ago? _____ Are they currently fleeing? Yes ☐ No ☐

APPENDIX I: RESERVED

APPENDIX J: HMIS DATA QUALITY PLAN

HMIS Quality Assurance (QA) Plan Overview:
The following are policies and procedures the CoC will implement to ensure the data integrity of agencies/programs.

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

- All names will be accurate
- Blanks or 'unknown' entries in required data fields will not exceed 5% per month
- All users should aim to have 0 % of null data
- All services provided will be compatible with the standard services of the program
- In all reports of shelter provided for a client, the client must be eligible to receive shelter services from the listed provider

Procedure: The HMIS CoC 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. When patterns of error have been discovered, users will be required to correct data entry and will be monitored for compliance.

1.) The HMIS CoC Administrator(s) shall generate data reports showing clients with missing *Universal Data* elements and clients with missing *Program Data* elements.
2.) The HMIS CoC Administrator(s) will generate Data Completeness reports, and submit to Agency Administrator findings and timelines for correction.
3.) The HMIS CoC Administrator(s) reports (e.g., Missing Universal and Program Data elements) will generate emails to all users with data entered or updated within the last 30 days from when the report is run, with a list of clients with missing data and the elements that are absent.
4.) The HMIS CoC Administrator(s) can also generate custom report for funded programs filtered on required fields for program types.
5.) The HMIS CoC Administrator(s) can rerun reports for errant agencies/programs and follow up with Agency Administrator, if necessary.
6.) The data is to be corrected within 14 calendar days and reviewed to make sure corrections are made appropriately.
7.) Users can monitor their own data by running Entry/Exit Reports, APR Reports, Clients Served Reports or Daily Bed Reports to ensure that they do not have any "null" or missing data in both the *Universal* and *Program* elements.

APPENDIX K: HMIS MONITORING CHECKLIST

SOUTH CAROLINA INTERAGENCY COUNCIL ON HOMELESSNESS

SCICH HMIS Monitoring Checklist

Date: _____

Agency:_____

Monitors: _____

Monitoring is conducted on all agencies that participate in the Homeless Management Information Systems to ensure that all agencies are taking the necessary precautions to ensure that client data is secure and protected at all times.				
Requirement	Description	2=Fully Met/Yes	1=Partially Met/80% or higher	0=Did Not Meet/80% or lower/No
Policies & Procedures	Does the agency have a copy of the latest Policies and Procedures manual with all amendments?	Yes		No Agency does not have a hard or electronic copy readily available to users.
Data Collection	Does the agency have a data collection form and/or protocol that captures universal and program specific (where applicable) data elements?	Yes		No– The agency does not have a data collection form or protocol.
	Agency is capturing universal data on all clients.	Yes		No
	Agency is capturing program level data as required.	Yes		No
	All users have been trained on revised protocols and any new data standards by the system administrator.	Yes	No- ___/____ users have been trained.	No- ___/____ users/ or no users have been trained.
	All programs have a 96% or higher data quality score.	Yes	No- ___/____ programs have a 96% or higher data quality score.	No- ___/____ or no programs have a 96% or higher data quality score.
	All users understand that clients can't be denied services based on HMIS participation.	Yes	No- ___/____ users gave the correct answer.	No- ___/____ users gave the correct answer.
Privacy Statement	Does the agency have the Privacy Notice posted in a common area where all clients can see it? *Appendix F	Yes		No
	Hard and/or electronic copies of the Privacy Notice are available. *Appendix F	Yes		No
	Does the agency have a privacy policy? *Appendix E	Yes		No
	Hard and/or electronic copies of the privacy policy are available. *Appendix E	Yes		No

User Authentication	All users abide by the HMIS policies for unique user names and password.	Yes	No-___/____ users abide by the policy.	No-___/____ users abide by the policy.
	All users know not to share usernames and passwords.	Yes	No- ___/____ users gave the correct answer.	No- ___/____ users gave the correct answer.
	All users do not have their usernames and password in a public place. (ie. Sticky notes on monitor)	Yes	No-___/____ users do not have their usernames and password in a public place.	No-___/____ users do not have their usernames and password in a public place or everyone has their credentials in a public place.
PPI Data	Does the agency have procedures in place to protect hard copy and/or electronic PPI information generated from or for the HMIS?	Yes		No
	Hard copies are stored in locked drawer or office?	Yes		No
	All staff have received training on hard copy data protections?	Yes	No-___/____ users have received training.	No-___/____ users/ no users have received training.
	Sampling of no less than 10 clients			
	Any PPI data entered after expiration of the ROI?	Yes	Yes- ___/____ ROIs were expired	No- __/___ ROIs/all ROIs were expired
PPI Storage	Does the agency dispose of or remove identifiers from a client record after a specified period of time? (Minimum standard: 7 years after PPI was last changed if record is not in current use.)	Yes		No
	Does the agency have policies and procedures to dispose of hard copy PPI or electronic media?	Yes		No
	All users are trained on the proper disposal of data?	Yes	No-___/____ users have received training.	No-___/____ users have received training.
Virus Protection	Do all computers have virus protection with automatic update?	Yes	No-___/____ computers have virus protection with automatic update.	No-___/____ computers have virus protection with automatic update.
	Auto-update turned on.	Yes		No
*Not scored	Virus software and version: _____ Person responsible for monitoring/updating: _____			

Firewall	Does the agency have a firewall on the PC, network and/or workstation(s) to protect the HMIS systems from outside intrusion?	Yes	[redacted]	No
*Not scored	Setup: ☐ Individual work station ☐ Network Version: _____			
Workstation Authentication	Does the agency have a secure internet connection?	Yes	[redacted]	No-___/____ computers have a secure internet connection
* Not scored for 2019 monitoring	The agency has a policy and has trained all users on internet and data security if work is taken outside of the office. ☐ Yes ☐ No			
	Does your agency have a Chief Privacy Officer that is in charge of privacy and yearly data audits? ☐ Yes ☐ No If yes, please list who. _____			
	All users understand that if approached by law enforcement that information on clients that is in HMIS or the location of clients cannot be disclosed without a court order. The HMIS administrator should be contacted in the event this happens. ☐ Yes ☐ No			
Physical Access	All HMIS workstations are in secure locations or are they manned at all times if they are in publicly accessible locations.	Yes	No-___/____ workstations are in a secure location or manned at all times.	No-___/____ workstations are in a secure location or manned at all times.
	All workstations have password protected workstations with password protection screen saver set at 10 minutes of less.	Yes	No-___/____ workstations are setup with the security features.	No-___/____ workstations are set-up with the security features.
	All printers are accessed with access codes or printers are in the same room as the user.	Yes	No-___/____ printers follow the stipulations.	No-___/____ printers follow the stipulations.
Accommodations	The agency has a protocol in place to assist clients who are not English proficient or have visual disabilities?	Yes	[redacted]	No
	All user have been trained on the protocol or how to assist clients who are not English proficient or have visual disabilities.	Yes	No-___/____ users have received training.	No-___/____ users have received training.
Score	**Total:** **____/60**	• 48+ points= Passed/no additional monitoring is needed for the year. • >48 points= Failed/Additional monitoring for the year is needed		
Notes				
	Additional Monitoring Needed: ☐ Yes ☐ No Monitor Signature: _____ Agency Staff Signature: _____			

APPENDIX L: MEMORANDUM OF AGREEMENT

MEMORANDUM OF AGREEMENT AND RELEASE TO SHARE IDENTIFYING INFORMATION WITH ORGANIZATIONS NOT AFFILIATED WITH HMIS

1) Patient Name:_____
2) Specific names of the programs or entities permitted to disclose information:

_____

_____

3) Specific names of the programs or entities receiving disclosed information:

_____

_____

The CoC, HMIS Lead Agency, and Third Party_____ (the "Parties") acknowledge the benefits of sharing client information to improve coordination and ability to provide service. The Parties agree to abide by, and be fully bound by, the HMIS Policies and Procedures, HMIS Privacy Policy, Confidentiality Guidelines, HMIS Code of Ethics, HMIS Data Quality Plan in sharing information, and 42 C.F.R. Part 2.

Print Name of Third Party

The Parties acknowledge that this release is valid ONLY for client information obtained through the client's or guardian's written consent, NOT implied consent. The above Third Party assures the CoC, HMIS Lead Agency, and the client/parent/guardian that it will maintain the confidentiality, security, and integrity of the client's personal information, pursuant to the Children's Online Privacy Protection Act of 1998. Further, it confirms it will not reproduce and/or distribute any disclosed information to another third party. The Parties must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the disclosure's intended purpose. Accordingly, the Parties acknowledge and guarantee that the above Third Party is capable of maintaining the confidentiality, security, and integrity of the client's personal information. The above Third Party acknowledges its duty to report, as soon as known, any use or disclosure not provided for in this agreement.

The Parties further recognize that, for this form to be valid, the client/parent/guardian must also have signed Appendix D, the *Acknowledgment of Receipt of Notice of SC-211 Homeless Management Information System (HMIS) Privacy Practices and Release of Information*. This document should be reviewed and signed by the HMIS CoC Administrator prior to release, in accordance with Section 8.8 of the HMIS Policies and Procedures.

X_____ X_____
Print CoC Administrator Name CoC Administrator Signature

X _____ X_____
Print HMIS Leady Agency Representative Name HMIS Lead Agency Representative Signature

X _____ X_____
Print Third Party Representative Name Third Party Representative Signature

FOR USE ONLY IF DISCLOSING SUBSTANCE USE DISORDER INFORMATION:

Explicit description of the substance use disorder information to be disclosed: _____

_____

_____

_____

I, _____, am aware that, by signing this document, I am consenting
Print Client Name
to the above organizations (the Parties) sharing my personal information. I am aware that my information will be shared with an organization not affiliated with HMIS, but which maintains the same standards of confidentiality and privacy. I understand that the shared information may include my: (1) full name; (2) social security number; (3) date of birth; (4) gender; (5) race; (6) ethnicity; (7) mental health assessment/progress; (8) medical/health information; (9) financial and work/residential information; (10) substance abuse assessment/progress; and (11) needs and services provided. I confirm my understanding that, upon my request, I must be provided with a list of entities to which my information has been disclosed. I, _____, acknowledge that, by signing this document, I have received all confidentiality policies and have signed Appendix D, or *Acknowledgement of Receipt of Notice of SC-211 Homeless Management Information System (HMIS) Privacy Practices and Release of Information*.

I further acknowledge that I may revoke this consent at any time. I understand that treatment or enrollment in this program or affiliated programs is not conditioned on whether I sign this consent form. I understand I am required to receive a copy of this signed form.

I understand that this information is to be released for the purpose of continuity of care/case management and is valid for one year unless otherwise specified.

X _____ Date:_____
Client/Parent/Guardian Signature

THIS BOX FOR OFFICIAL USE ONLY

I have reviewed this document and acknowledge that all necessary information is complete.

X _____ X_____
Print HMIS CoC Administrator Name HMIS CoC Administrator Signature

Date:_____

APPENDIX M: FORM ACKNOWLEDGEMENT

SC-211	**HMIS Privacy Policy and Code of Ethics Acknowledgement**

ACKNOWLEDGEMENT

MY SIGNATURE BELOW ACKNOWLEDGES THAT I HAVE RECEIVED A COPY OF, READ, AND REVIEWED THE HMIS PRIVACY POLICY AND CODE OF ETHICS GOVERNING MY USE OF THE SC-211 HOMELESS MANAGEMENT INFORMATION SYSTEM (COLLECTIVELY, THE "MATERIALS"). I FURTHER ACKNOWLEDGE AND UNDERSTAND THAT IT IS MY RESPONSIBILITY TO ABIDE BY ALL RULES AND REQUIREMENTS SET FORTH IN THE MATERIALS, AND ANY OTHER POLICIES THE MATERIALS MAY REFERENCE, AND ANY LATER VERSIONS, REVISIONS, AND/OR MODIFICATIONS TO THE MATERIALS.

_____ _____
Signature Date

_____ _____
Print Name Position

Return signed copy to [appropriate individual or position to record acknowledgements].