

## 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 Systems Administrator:**

Scott Sox - MACH HMIS System Administrator  
803-733-5103  
[ssox@uway.org](mailto:ssox@uway.org)

### COMPLETE THE FOLLOWING:

Agency Name: \_\_\_\_\_

Employee Name & Position Title: \_\_\_\_\_

Employee Email Address: \_\_\_\_\_

Employee Contact Number: \_\_\_\_\_

### ACCOUNT TYPE (check one):

- Agency Administrator** – have full access to all aspects of ServicePoint. They can also update their agency profile, change user access rights and user passwords, and delete client records.
- Case Manager** – have full access to all aspects of ServicePoint, but have no administrative rights.
- Volunteer** – can enter data, assign beds, and log client referrals. Regarding client demographic data already in the system, they can only view a client’s names, date of birth, and SSN.

### 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 (page 3) 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 (page 3).
- I have read and understood the HMIS Privacy Policy (pages 4 - 12).
- I have read and understood the HMIS Code of Ethics (page 13).

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

<hr/>	<hr/>
Employee's Signature	Date
<hr/>	<hr/>
Supervisor's Signature	Date
<hr/>	<hr/>
CoC HMIS System Administrator Signature	Date

## 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.

Revised and Approved: February 25, 2021



2004 HMIS Data and Technical Standards Final Notice:

<https://www.hudexchange.info/resource/1318/2004-hmis-data-and-technical-standards-final-notice/>

## 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**

Revised and Approved: February 25, 2021

4



2004 HMIS Data and Technical Standards Final Notice:

<https://www.hudexchange.info/resource/1318/2004-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).

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

Revised and Approved: February 25, 2021

5



2004 HMIS Data and Technical Standards Final Notice:

<https://www.hudexchange.info/resource/1318/2004-hmis-data-and-technical-standards-final-notice/>

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:

Revised and Approved: February 25, 2021

6



2004 HMIS Data and Technical Standards Final Notice:

<https://www.hudexchange.info/resource/1318/2004-hmis-data-and-technical-standards-final-notice/>

- 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

Revised and Approved: February 25, 2021



2004 HMIS Data and Technical Standards Final Notice:

<https://www.hudexchange.info/resource/1318/2004-hmis-data-and-technical-standards-final-notice/>

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 CHO's 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**

Revised and Approved: February 25, 2021



2004 HMIS Data and Technical Standards Final Notice:

<https://www.hudexchange.info/resource/1318/2004-hmis-data-and-technical-standards-final-notice/>



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:

Revised and Approved: February 25, 2021



2004 HMIS Data and Technical Standards Final Notice:

<https://www.hudexchange.info/resource/1318/2004-hmis-data-and-technical-standards-final-notice/>

- 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:

Revised and Approved: February 25, 2021

10



2004 HMIS Data and Technical Standards Final Notice:

<https://www.hudexchange.info/resource/1318/2004-hmis-data-and-technical-standards-final-notice/>

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.

Revised and Approved: February 25, 2021

11



2004 HMIS Data and Technical Standards Final Notice:

<https://www.hudexchange.info/resource/1318/2004-hmis-data-and-technical-standards-final-notice/>

## HMIS PRIVACY STATEMENT

<p><b>SUMMARY OVERVIEW</b></p>	<p>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).</p> <p>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.</p> <p>The SC CoC’s CES is used to connect individuals and families at risk of or experiencing homelessness to the services they need.</p> <p>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.</p> <p>This organization may use or disclose information from the SC HMIS and / or the SC CoC’s CES under the following circumstances:</p> <ul style="list-style-type: none"> <li>• To provide or coordinate services for an individual or household;</li> <li>• For functions related to payment or reimbursement for services;</li> <li>• To carry out administrative functions;</li> <li>• When required by law;</li> <li>• For research and / or evaluation; or</li> <li>• For creating deidentified data.</li> </ul>
<p><b>USES, RISKS, PROTECTIONS</b></p>	<ul style="list-style-type: none"> <li>• Information you provide to this organization will be entered into the HMIS and shared with partner organizations unless you opt-out.</li> <li>• 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.</li> <li>• 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.</li> <li>• Your personal information that is in the HMIS will not be shared with any other government organizations except as required by law.</li> <li>• Personally Identifying Information (PII), such as names, birthdays, and social security numbers, will be available to partner organizations in the HMIS for seven years.</li> <li>• 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.</li> <li>• Your data is protected by legal agreements signed by Users of the HMIS and by electronic encryption of your personal information.</li> </ul>
<p><b>YOUR RIGHTS &amp; CHOICES</b></p>	<ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> </ul>
<p><b>CONTACT INFORMATION</b></p>	<p style="text-align: center;">Midlands Area Consortium for the Homeless (MACH) Continuum of Care          1818 Blanding Street, Columbia, SC 29201          803-733-5101          lhopkins@uway.org          midlandshomeless.com</p>

## **HMIS 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 breach.

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.*