ATTACHMENT A
CONFIDENTIALITY GUIDELINES

The CHO agrees to abide by all present and future federal and state laws and regulations and with all United Way of the Midlands procedures and policies relating to the collection, storage, retrieval, and dissemination of client information for the South Carolina Information Collaborative (SCIC) and will only release confidential client information 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 records and 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 SCIC and complies with the regulations governing the HMIS.

2. The CHO will provide a verbal explanation of the SCIC 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 CHO's 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 SCIC Privacy Policy, available to any client requesting a copy.[1]

4. The CHO agrees to limit access to information furnished by the SCIC 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 SCIC. All such employees will be required to sign a statement of confidentiality, which includes a pledge of compliance (**Attachment B**). Each statement of confidentiality will be forwarded to and maintained by United Way of the Midlands. 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 further agrees to furnish to United Way of the Midlands the names of all staff members who have access to SCIC information and certify that such staff is competent to have access to this information according to the provisions of this agreement. United Way of the Midlands may, at its option, disapprove access of the system to any individual.

7. 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.

8. The CHO Executive Director must accept responsibility for the validity of all records entered by their agency. The Executive Director may designate an immediate subordinate staff member with supervisory responsibilities for verifying the accuracy of information. The CHO will provide United Way of the Midlands with the name(s) and title(s) of the staff member(s) authorized to supervise data entry personnel.

9. United Way of the Midlands reserves the right to immediately suspend furnishing information covered by terms of this Agreement to the CHO when any terms of this Agreement are violated or are suspected of being violated. Upon receipt of satisfactory assurances that such violations did not occur or that such violations have been fully corrected or eliminated, United Way of the Midlands in its sole discretion may resume furnishing such information.

[1] SCIC Privacy Policy

ATTACHMENT B

REQUEST FOR SCIC USER ACCOUNT

Homeless Management Information System

Account Type (check one):

[ ] Case Manager

[ ] Volunteer

[ ] Agency Administrator

This request/certification must be completed by all users and existing users on at least an annual basis.

Please visit:
https://www.cognitoforms.com/UnitedWayOfTheMidlands1/RequestForm

1. Select "New User Request" from the drop-down.
2. Complete, sign, and upload this document.
3. If this is an annual recertification for an account that already exists, enter a note in the "Additional Information" section.

Agency Administrator users have full access to all aspects of ServicePoint, and in addition, can update their agency profile, change user access rights and user passwords, and delete client records.

Case Manager users have full access to all aspects of ServicePoint, but have no administrative rights.

Volunteer users can enter data, assign beds, and refer clients, but can only view name, date-of-birth, and SSN of client data.

Please complete the following:

Employee Name:

_____

Employee Email Address:

_____

Agency Name and Telephone 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 SCIC (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 System Administrator for their temporary password.
- All End Users must obtain and review a copy of the SC-HMIS Policies and Procedure to include Privacy Statement, Security, and Data Quality sections.
- After reviewing the Confidentiality Guidelines **(Attachment A)** please sign the Confidentiality and Responsibility Certification **(next page).**

SCIC USER

CONFIDENTIALITY AND RESPONSIBILITY CERTIFICATION

I have read the Confidentiality Guidelines and I agree to maintain strict confidentiality of information obtained through the South Carolina Information Collaborative (SCIC). This information will be used only for legitimate client service and administration of the above named agency. Any breach of confidentiality will result in immediate termination of participation in the SCIC.

Initial each item

____ I understand that my username and password are for my use only (or job-sharing counterpart).

____ 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 SCIC are authorized users and the clients to whom the information pertains.

____ 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 SCIC whatever their role or position.

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

____ I understand that once hard copies of SCIC 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 (see below).

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

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

I understand and agree to the above statements.

Employee's Signature_____ Date: _____

Supervisor's Signature_____ Date: _____

Executive Director's Signature: _____ Date: _____

_____
System Administrator or HMIS Consultant