

## SC HMIS P&P Changes

1. **2 South Carolina HMIS Steering Committee**
  - Clarified South Carolina HMIS Steering Committee meeting frequency, committee leadership roles, and voting process.
2. **4.1 Contributory HMIS Organization**
  - Clarified HMIS access prioritization– Priority will be given to 1) shelters – any facility with overnight sleeping accommodations where the primary purpose of which is to provide temporary shelter for the homeless in general or for specific sub-populations, 2) permanent housing providers servicing the homeless population, 3) service agencies targeting the homeless population, 4) other agencies serving at-risk populations.
  - Expanded the DV section to include that they are encouraged to use a comparable HMIS database for data entry.
  - Included HMIS Lead information for each CoC.
3. **4.2 Agreements to Participate**
  - Updated section to include wording that the MOA is to be used statewide by all four CoCs and that no other document can be substituted for the MOA.
  - Updated MOA (**Appendix B**) will be sent to all current and new HMIS agencies.
4. **4.3 Terms of Participation**
  - Expanded to include wording that agencies are prohibited from directly contacting the HMIS vendor (WellSky) to request custom database work. All requests must be made through the SC HMIS Steering Committee via the local HMIS Lead staff.
  - This section also now includes the approval of an agency to participate in HMIS is at the discretion of the CoC.
5. **4.4 HMIS Project Set-Up (new section)**
  - Includes required information needed by the HMIS Lead to setup a new project on HMIS including Provider profile information, Standards information, Visibility information, Services provided, Module access settings, Assessments needed, Assessment display settings.
6. **4.4.1 Provider & Project Naming Convention (new section)**
  - This section created a standard naming convention to be used by all four CoCs, which helps to accurately convey the CoC where the project is located, and the type of service provided by the project. Projects are to be named with the CoC HMIS Acronym – Project Name – Project Funding Source – Project Type.
7. **5.1 Securing Access, Usernames, and Passwords**
  - Added wording stating that HMIS Lead agencies reserve the right to assess a fee per license based on availability or limited resources.
  - Added wording that all users must complete training prior to HMIS access, which covers accessing WellSky’s Community Services, maintaining high data quality, and ensuring security/privacy. As part of the training, HMIS Lead agencies reserve the right to assess fees for training. The training is also to be provided by the HMIS Lead or the HMIS Lead contractor.
  - Added wording that HMIS users must sign the HMIS User Agreement (**Appendix C**), which also may be required to be signed by the user’s immediate supervisor if required by the CoC.
  - Added requirements of HMIS passwords. They must be at least 8 characters, a mix of numbers and symbols and avoid repeating letters/numbers. Passwords cannot be

shared or written down and stored in a publicly accessible location. Users must not store their HMIS passwords on their computer for easier login. Passwords expire every 45 days. Users may not use the same password consecutively. Passwords cannot be re-used until two password selections have expired. If a User unsuccessfully attempts to log-on three times, the system will force the User to reset their own password or have their password reset by the HMIS System Administrator.

- Added section **10** requiring users to login to HMIS once every 30 days or risk losing their HMIS license. CoCs reserve the right to terminate the license and/or charge an agency a penalty fee for non-use of the system at their discretion.

#### 8. **5.2 User Conflict of Interest (new section)**

- Added wording stating that current clients, or volunteers who were clients receiving homeless services within the last six months, cannot be granted access to the HMIS. Former clients who have been hired by an agency to perform HMIS duties will be granted access with approval from the local HMIS Lead Agency. Additionally, all Users cannot modify client records for which an obvious conflict of interest exists.
- All Users must sign the HMIS User Agreement, which includes a statement describing this limitation, and report any potential conflict of interest to their designated agency HMIS Contact. The System Administrator may run the audit report to determine if there has been a violation of the conflict-of-interest agreement.

#### 9. **5.4 Violations and Non-Compliance Policy (new section)**

- Added wording that users are required to follow the Policies and Procedures as defined in the document. If there are violations, users and or agencies will face repercussions.
- Added a list of websites where users can find the P & P.
- Included a copy of the HMIS Violations and Non-Compliance Policy (**Appendix G**). Violations of the P & P will be investigated and enforced.

#### 10. **6.1 Ownership of Data**

- Expanded section to include wording that the data may also be shared with organizations outside of HMIS, pursuant to an executed Research Agreement or with the SC Revenue and Fiscal Affairs office for research purposes.
- Expanded section to include information on how the data is backed up, where it is stored (United Way of the Midlands), and how the data is secured. The data back-up is overwritten on a weekly basis and historical back-ups are not held indefinitely.

#### 11. **6.22 Privacy Policy**

- Added wording that the HMIS Privacy Policy cannot be modified in any form and that each CoC must use the version that is listed in the P & P (**Appendix D**).
- Expanded section to include information on how the data is protected while allowing for reasonable, responsible, and limited uses and disclosures of data in following the 2004 HMIS Data and Technical Standards Final Notice.
- Expanded section to include information on how the data can be used or disclosed and how clients can access their information.
- Removed the requirement of the Release of Information for data sharing.

#### 12. **Merging Duplicate Client Records**

- Expanded section to include information on how client records will be merged if one of the clients originated in another CoC. In these cases the SA from the CoC conducting the merge must contact the SA from the other CoC to let them know a merge needs to take place. Once the merge is completed, it is recommended that the SA email each agency that had

provided services to the client within the past three years so the agency can update their records.

- Locked records will remain locked and cannot be merged.

### **13. 6.5.2 Data Accuracy & 6.5.3 Data Timeliness**

- Agencies/projects are required to have a 96% or above “non-null” data quality rate. CoC’s reserve the right to levy penalties or fines for not adhering to Data Accuracy standards.
- Data is to be entered into HMIS within 72 hours of when it is collected. CoC’s reserve the right to levy penalties or fines for not adhering to Data Accuracy standards.

### **14. Data Imports (new section)**

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

### **15. 6.8 Procedure to Follow if Approached by Law Enforcement for Client Information in HMIS (new section)**

- Added wording that the agency and user must contact the HMIS Administrator and CoC Leadership (as defined locally by each CoC) whenever there is a request from Law Enforcement to access a client’s information within HMIS.

### **16. Device Security**

- Added wording stating that users are required to follow the SC HMIS Remote Access Guidelines (**Appendix K**).

### **17. Data Security**

- Added wording that data within the system must be kept for seven years.
- Added wording that users can now reset their own passwords when they get locked out due to three unsuccessful login attempts by clicking on the “Forgot Password” button.
- Added wording that any PII data stored on a device or external media must be encrypted in accordance with current industry standards.

### **18. Client Data Sharing**

- Added wording of the types of data, levels of sharing, and typical sharing settings.
  - Added “Household composition” to the types of data HMIS contains.
  - Added wording that data is shared globally, which is allowed for by the uses and disclosures covered in the HMIS Privacy Policy.
  - Added additional wording stating that Name, SSN, Veteran Status is shared globally to ensure users are able to complete a client search and identify if a record exists in HMIS already.
  - Added wording to clarify that agencies that primarily assist children are only set to share client record (Name, SSN, Vet status) data and not full client profiles.

### **19. 7.4 Client Record Information (Name, SSN, Veteran Status) on Client Profile**

- Added wording clarifying that Client Record data is located on the Client Profile tab and is shared Globally to allow for de-duplication of client records.
- Clarified that no other assessment information is to be visible on the Client Profile tab.

### **20. 7.5 Aggregate Data Sharing and Release**

- Added wording that reports may be made public provided the reports only contain aggregate data.
- Client level information may be shared for research, planning, and coordinated entry purposes. If client level data is being requested by a research organization or university, with the exception of Revenue and Fiscal Affairs (RFA), a signed Research Agreement (**Appendix L**), must be in place.

**21. 7.5.1 Release of Data for Grant Funders (new section)**

- Added wording that a funding agency should not expect HMIS access unless there is a MOA in place between the funder and the HMIS Lead. The HMIS Lead must then present this unique MOA agreement to the SC HMIS Steering Committee for approval.

**22. 7.5.2 Statewide Reporting (new section)**

- Added wording stating that when aggregate statewide HMIS data is requested, all four CoCs must agree on the scope, data extraction/compilation, and review of the findings before the results are released.

**23. 7.6 Data Extracts**

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

**24. 8.1 Technical Support**

- Added wording that users should contact the HMIS Lead through the communication method established by the HMIS Lead (ticketing system, HMIS Help Desk).

**25. 8.2 HMIS Monitoring**

- Added wording that the SA has the right to conduct monitoring of agency and user compliance with the policies and procedures documented in the SC HMIS P & P Manual.
- Added wording that the HMIS Monitoring Checklist (Appendix M) represents a baseline for what SAs should consider when conducting HMIS monitoring. Each CoC reserves the right to add-on to the checklist, but do not have permission to remove any items being evaluated.
- Added wording that CoCs reserve the right to conduct their HMIS monitoring in accordance to locally defined priorities as decided by their local HMIS Committee or CoC Leadership.
- Added wording that if an agency does not pass their monitoring, a corrective action plan will be developed between the agency and the HMIS Lead/HMIS Contractor. The corrective action plan is to be completed by the agency within 90 days of the delivery of the corrective action plan from the HMIS Lead/HMIS Contractor.

**26. 8.3 Vendor Requirements (new section)**

- Added wording detailing the requirements of WellSky as the HMIS Vendor of ServicePoint. These details include their obligation to maintain security (physical security, firewall protection, user authentication, application security, database security), performance (technical performance, hardware disposal), and support of the database system (technical support).

27. **8.4 Disaster Preparedness (new section)**

- Added wording detailing how WellSky will provide disaster recovery services. The Disaster Recovery Plan includes information on nightly database backups, offsite storage of backups, 7-day backup history stored locally on instantly accessible RAID storage, 1-month backup history stored offsite, 24x7 access to WellSky's emergency line to provide assistance related to "outages" or "downtime", and 24 hours data backed up locally on instantly accessible disk storage.

28. Updated **Memorandum of Agreement (Appendix B)**

29. Updated **HMIS User Agreement Confidentiality and Responsibility Certification (Appendix C)**

30. Updated **South Carolina HMIS Privacy Policy (Appendix D)**

31. Updated **Confidentiality Guidelines (Appendix E)**

32. Updated **Code of Ethics (Appendix F)**

33. Updated **South Carolina Statewide HMIS Violations and Non-Compliance Policy (Appendix G)**

34. Updated **Privacy Statement (Appendix H)**

35. Updated **HMIS Data Quality Plan (Appendix J)**

36. **Added SC HMIS Remote Access Guidelines (Appendix K)**

37. **Added SC HMIS Committee Research Agreement (Appendix L)**

**38. Updated SC HMIS Monitoring Checklist (Appendix M)**