WESTCHESTER COUNTY CONTINUUM OF CARE
PARTNERSHIP TO END HOMELESSNESS

c/o WC DCMH
112 East Post Road, 2nd Floor
White Plains, NY 10601
(914) 995-5220

HMIS Agency Participation Agreement

	Westchester County Department of Social Services
Partner Agency Name	HMIS Lead Agency Name

I. BACKGROUND AND PURPOSE

The Homeless Management Information System (HMIS) is the information system designated by the Westchester County Continuum of Care Partnership for the Homeless (CoC Partnership) to comply with HUD's data collection, management, and reporting standards and used to collect client-level data and data on the provision of housing and services to homeless individuals and families and persons at risk of homelessness.

The U.S. Department of Housing and Urban Development (HUD) and other planners and policymakers at the federal, state and local levels use aggregate HMIS data to obtain better information about the extent and nature of homelessness over time. Specifically, an HMIS can be used to produce an unduplicated count of homeless persons, understand patterns of service use, and measure the effectiveness of homeless programs. Through the HMIS, CoC programs and clients benefit from improved internal and external coordination that guides service and systems planning. A robust HMIS also helps communities engage in informed advocacy efforts, including the pursuit of policies that result in targeted services. Analysis of information gathered through HMIS is critical to accurately calculate the size, characteristics, and needs of different subpopulations. Additionally, use of the HMIS by agencies not funded by HUD provides benefits to both these agencies and the homeless provider community at large, including the avoidance of service duplication through the sharing of client data. HMIS participation also positions agencies for future funding, as many private foundations now require it.

II. GENERAL PROVISIONS

A. The CoC Partnership has designated Westchester County Department of Social Services (DSS) as the HMIS Lead Agency. All homeless assistance and homelessness prevention service providers in this CoC are eligible to become HMIS Partner Agencies, except for domestic violence providers covered by the Violence Against Women Act (VAWA). The parties share a common interest in serving the homeless population and those at risk of becoming homeless while reducing the current number of homeless in the CoC jurisdiction. The purpose of this agreement is to set out the provisions for the implementation, maintenance, coordination and operation of the HMIS. DSS – in coordination with its authorized agents, including the HMIS Software Provider and HMIS Administrator – is responsible for administering the HMIS on behalf of the CoC, including the implementation, management, training, maintenance, support and enhancement of the HMIS software. The Partner Agency is responsible for entering client data in the HMIS according to program requirements. Detailed responsibilities are listed in sections below.

B. The Agency Participation Agreement (APA) addresses the respective responsibilities of DSS and the Partner Agency for ongoing HMIS service and activities. The specific responsibilities of the parties to this agreement for the confidentiality, reporting requirements, training, policies and procedures, hardware and software for the HMIS are clearly defined herein to ensure an effective, efficient and secure system. All addendums referenced in this agreement are also part of the agreement. DSS will abide by all applicable laws, and the Partner Agency will be expected to do the same.

III. DSS DUTIES AND RESPONSIBILITIES

c/o WC DCMH
112 East Post Road, 2nd Floor
White Plains, NY 10601
(914) 995-5220

HMIS Agency Participation Agreement

DSS will:

A. GENERAL

1) In consultation with the CoC Partnership, select the HMIS Software Provider, define the HMIS program and implement its standards, promote awareness of the program to all interested parties and monitor the program's successes and failures in order to validate its effectiveness.
2) Hold the Partner Agency, and its agents, harmless and indemnify it from any and all damages, liabilities, claims and expenses that may be claimed by any third parties arising from DSS's conduct under this agreement.
3) Be the sole liaison between the Partner Agency and the HMIS Software Provider; user questions concerning the software are to be directed only to DSS.
4) Develop, implement and maintain privacy, confidentiality and security protocols for the HMIS in consultation with the CoC Partnership.
5) Provide standardized HMIS training and technical assistance to all Partner Agencies.
6) In collaboration with the HMIS Software Provider, take all necessary precautions to prevent any destructive or malicious programs from being introduced to the HMIS and, through it, to the Partner Agencies. DSS will employ all appropriate measures to detect virus infection and all appropriate resources to efficiently disinfect any affected systems as quickly as possible.
7) Notify the Partner Agency of HMIS failure, errors and/or problems immediately upon discovery.
8) Provide technical assistance during normal business days, with the exception of federal and scheduled holidays.
9) Provide all other reasonably expected activities regarding the operation of the HMIS.

B. PRIVACY, CONFIDENTIALITY AND SECURITY

1) Maintain all client-identifying information in strictest confidence. DSS may suspend HMIS access to any user or Partner Agency for the purpose of investigating suspicion of breached confidentiality.
2) Contract with the HMIS Software Provider to maintain and administer central and backup server operations including security procedures and daily system backup to prevent the loss of data.
3) Designate the HMIS Lead Security Officer in the HMIS Lead Security Certification document, which must be updated at least annually. The contact information is incorporated into the Security Provisions by reference. The duties of the Security Officer must be included in the individual's job description or HMIS Lead Security Certification, and signed by the Security Officer to indicate understanding and acceptance of these responsibilities. These duties include, but may not be limited to:
   - With the HMIS Administrator, review the Security Provisions annually and at the time of any change to the security management process, the HMIS software, the methods of data exchange, and any HMIS data or technical requirements issued by HUD. In the event that changes are required to the HMIS Security Provisions, work with the HMIS Administrator to develop recommendations to the CoC Partnership for review, modification and approval.
   - Annually review the HMIS Lead Security Certification document, test the HMIS Lead security practices for compliance, and work with the HMIS Administrator to coordinate communication with HMIS Software Provider to confirm security compliance.
   - Using the HMIS Lead Security Certification document, certify that the HMIS Lead adheres to the Security Provisions or develop a plan for mitigating any shortfall, including milestones to demonstrate elimination of the shortfall over as short a period of time as is possible.

c/o WC DCMH
112 East Post Road, 2nd Floor
White Plains, NY 10601
(914) 995-5220

HMIS Agency Participation Agreement

- Implement any approved plan for mitigation of shortfalls and provide appropriate updates on progress to the CoC Partnership.
- Respond, in cooperation with the HMIS Administrator, to any security questions, requests, or security breaches to the CoC Partnership, and for communicating security-related HMIS information to the organization's end users.

4) Ensure the HMIS Lead Security Officer and any administrative user able to manage and access data from more than one Partner Agency undergo criminal background verification. Record of the completed background check (though not the results) is subject to inspection by the CoC. The HMIS Lead will hire individuals with criminal justice histories only to the extent the hire is consistent with any relevant hiring policies of DSS, unless the background check reveals a history of crimes related to identity theft or fraud. The HMIS Lead will manage the results of any background checks conducted on a case-by-case basis.
5) Monitor access to the HMIS in order to detect violations of information security protocols and maintain for inspection accurate logs of all changes made to the information contained within the database.
6) Issue user accounts, passwords and certificates of participation, when requested, for HMIS users, provided that:
   a) The Partner Agency has signed the APA;
   b) The Partner Agency has designated an HMIS Site Administrator;
   c) The HMIS Lead Agency has received signed User Agreements; and,
   d) The user has successfully completed HMIS user training, including any tests.
7) Periodically change Partner Agency passwords for security purposes and lock out user accounts after a specified period of inactivity.
8) Comply with the HMIS Privacy Policy and HMIS Data Sharing Policy and not release personally identifiable information to any person, agency or organization, unless allowed by the HMIS Privacy Policy.
9) Configure and maintain inter-agency data sharing options in HMIS.
10) Conduct Partner Agency site visits to ensure compliance with privacy and security protocols.

C. USER TRAINING AND PROGAM CONFIGURATION
1) Conduct training, including security training at least annually, for all HMIS users.
2) Authorize user access to HMIS in accordance with the HMIS policies and procedures.
3) Provide training materials, which may include user manuals, definitions and instructions, to each individual who attends the training event.
4) Configure Partner Agency programs according to the latest HMIS Data Standards, including related grants, services, assessments, housing units, and other applicable options in the HMIS software.
5) Provide additional trainings according to the user role, program type, or specific activities. These trainings may include web-based refresher courses in group or one-on-one format.

IV. Partner Agency DUTIES AND RESPONSIBILITIES

The Partner Agency will:

A. GENERAL
1) Strictly adhere to all policies and procedures contained in the APA, as it may be amended from time to time, and all of its appendices. A copy of this agreement can be found at http://programdesign.com/wiki/WCCOCH, and a signed hard copy will be provided to the Partner Agency.
2) Hold DSS, and its agents, harmless and indemnify it from any and all damages, liabilities, claims and expenses that may be claimed by any third parties arising from Partner Agency's conduct under this agreement.
3) Maintain at least 1 (one) active user account at any time.

c/o WC DCMH
112 East Post Road, 2nd Floor
White Plains, NY 10601
(914) 995-5220

HMIS Agency Participation Agreement

B. PRIVACY AND CONFIDENTIALITY

1) Comply with all federal and state laws and regulations, and with all HMIS policies and procedures (particularly the HMIS Data and Technical Standards Final Notice from July 2004, the HMIS Data Standards Revised Notice from March 2010 and subsequent revisions) relating to the collection, storage, retrieval, and dissemination of client data.
2) Comply with the HMIS Privacy Policy and the HMIS Data Sharing Policy.
3) Obtain client consent before any data is collected and shared. The consent can be:
   a) Inferred (baseline): The agency must post a visible HMIS Consumer Notice and HMIS Privacy Policy in a reception area or at each intake station.
   b) Informed Written (optional): The client may sign a release of information (ROI) form stored on location.
   c) Informed Verbal (optional): The client may give oral permission to Partner Agency personnel with written documentation of consent by witness.
4) Where informed written consent applies, utilize the HMIS Client Release of Information Form (ROI), or an alternative approved by DSS. With consent, the Partner Agency is authorized to share data until such time as the client withdraws consent, at which point the Partner Agency shall be responsible for ensuring the client's data entered thereafter is restricted from view. Collect and store records of any ROI authorizations for, at least, 3 (three) years.
5) Ensure no client is denied service for failure to release information for sharing purposes or refusal to answer informational questions not required for eligibility determination.
6) Take all necessary precautions to prevent destructive or malicious programs, including but not limited to viruses or spyware, from being introduced to any part of the HMIS, including users' computers. Employ appropriate measures to detect virus or spyware infection and deploy all appropriate resources to efficiently disinfect any affected systems as quickly as possible.

C. DATA QUALITY AND MONITORING

1) Fully comply with the latest HMIS Data Quality Plan. This plan is posted on the website, http://programdesign.com/wiki/WCCOCH, and available in hard copy upon request.
2) Enter data into the HMIS within the timeframe as specified in the Data Quality Plan. Timely data entry prevents duplication of client records and other shared transactions, such as enrollments and services. It also allows good quality data for both program-specific and aggregate reports. Partner Agencies and their HMIS users may be held liable in the event that a preventable duplication occurs as a result of missing, late or incomplete data entry. Repetitive lack of timely entry can result in official reports of concern and possible findings against the Partner Agency and could culminate in official penalties up to and including loss of project funding.
3) Collect all mandatory data elements, according to the data quality requirements.
4) Take all steps reasonably necessary to verify the information provided by clients, and to see that it is correctly entered into the HMIS by the Partner Agency user.
5) Immediately notify DSS when a programmatic, personnel or other issue arises that precludes the Partner Agency from entering the HMIS data within the allowed timeframe. By informing the DSS in a timely fashion, all parties can work together to craft an interim solution that is minimally disruptive to program operations and the HMIS as a whole.
6) Take reasonable steps to ensure that no profanity, offensive language, malicious information or discriminatory comments based on race, ethnicity, religion, national origin, disability, age, gender or sexual orientation are entered into the HMIS.
7) Do not upload material into the HMIS that is in violation of any federal or state regulations, including, but not limited to: copyrighted material, material legally judged to be threatening or obscene, and material known to the Partner Agency to be confidential trade secrets.

c/o WC DCMH
112 East Post Road, 2nd Floor
White Plains, NY 10601
(914) 995-5220

HMIS Agency Participation Agreement

8) Allow the DSS staff to conduct periodic monitoring and reviews of the original documentation in client files to ensure data accuracy. This monitoring is limited only to the client information relevant to HMIS data collection.

D. TRAINING

1) Ensure that each Partner Agency HMIS user attends the appropriate training, agrees to and signs the User Agreement, receives HMIS security training prior to being given access to HMIS and participates in security training at least annually.
2) Ensure that the Partner Agency program officers or designated HMIS site administrators attend any DSS-sponsored HMIS trainings, stay current with the HMIS policies and procedures, and relate news and updates to its HMIS users.
3) Assess the HMIS users' performance and refer for additional training as needed.

E. SECURITY

1) Limit HMIS access only to authorized users and follow all HMIS protocols for monitoring those users. DSS reserves the right to terminate access to any HMIS user who breaches client confidentiality or system security protocols.
2) Do not permit any person to enter or use the HMIS unless and until:
   a) The person has completed the required HMIS training;
   b) DSS has issued that person the appropriate user account and password; and,
   c) Both the APA and the User Agreement have been signed and returned to DSS.
3) Maintain copies of all User Agreements signed by Partner Agency personnel to whom user accounts have been issued.
4) Designate an HMIS Security Officer to be responsible for the implementation of the HMIS security provisions at the Partner Agency.
5) Fully comply with the HMIS Data Sharing Policy and the HMIS Privacy Policy.
6) Not release any HMIS data to any entity that is not part of the HMIS, unless such release is covered by the HMIS Data Sharing Policy or the HMIS Privacy Policy.
7) Develop an internal procedure to be used in the event of a violation of any of the HMIS security protocols.
8) Develop and adhere to local security standards that should include the following:
   a) Products: Physical security (door locks, computer screen view, local network passwords, firewall)
   b) People: Personnel security (authorized users only, local oversight of usage)
   c) Procedures: Organizational security (policies and procedures are in place)
9) Adhere to their own policies regarding conducting background checks and hiring individuals with criminal justice histories, as long as they comply with all relevant laws.
10) Notify HMIS Administrator within one business day of the separation of any employee who was a user of the HMIS. Notification should preferably occur by close of business on the day of employee separation.

V. PROPRIETARY RIGHTS OF CLIENTTRACK, INC.

A. The Partner Agency shall not give or share assigned passwords and access codes for HMIS with any other Agency, business, or individual.

B. The Partner Agency shall not cause in any manner, or way, corruption of HMIS.

VI. TERMS AND CONDITIONS

A. Neither the Lead Agency nor the Partner Agency shall transfer or assign any rights or obligations without the written consent of the other party.

c/o WC DCMH
112 East Post Road, 2nd Floor
White Plains, NY 10601
(914) 995-5220

HMIS Agency Participation Agreement

B. This Agreement shall be in-force until revoked in writing by either party provided funding is available.

C. This Agreement may be terminated immediately with cause.

The signature of the parties hereto indicates their agreement with the above terms and conditions.

_____
Agency NAME

_____ _____
Agency Representative Date

_____
Print NAME and TITLE

Westchester County Department of Social Services

_____ _____
Program Coordinator Date