

Westchester County Continuum of Care Partnership for the Homeless

Privacy and Security Provisions

For the Westchester Homeless Management Information System

Adopted by the WC CoC Partnership for the Homeless on 01/08/2014

Partner Agency Name	Westchester Co. Dept. of Social Services HMIS Lead Agency
---------------------	--

A. PRIVACY

- 1) DSS will 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) Partner Agencies will 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.
- 3) Partner Agencies will comply with these HMIS Privacy and Security Provisions and the HMIS Data Sharing Policy.
- 4) Partner Agencies will 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.
- 5) Where informed written consent applies, the Partner Agency will 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.

B. SECURITY

DSS will:

- 1) 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.
- 2) 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.
- 3) 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.
- 5) Periodically change Partner Agency passwords for security purposes and lock out user accounts after a specified period of inactivity.
- 6) Comply with these HMIS Privacy and Security Provisions and HMIS Data Sharing Policy and not release personally identifiable information to any person, agency or organization, unless allowed by these policies.
- 7) Configure and maintain inter-agency data sharing options in HMIS.
- 8) Conduct Partner Agency site visits to ensure compliance with privacy and security protocols.

Westchester County Continuum of Care Partnership for the Homeless

Privacy and Security Provisions

For the Westchester Homeless Management Information System

Adopted by the WC CoC Partnership for the Homeless on 01/08/2014

Partner Agencies will:

- 1) 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.
- 2) 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.
- 3) 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.
- 4) Maintain copies of all User Agreements signed by Partner Agency personnel to whom user accounts have been issued.
- 5) Designate a staff person to be responsible for the implementation of the HMIS security procedures at the Partner Agency level.
- 6) Fully comply with the HMIS Data Sharing Policy and the HMIS Privacy and Security Provisions.
- 7) 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 and Security Provisions.
- 8) Develop an internal procedure to be used in the event of a violation of any of the HMIS security protocols.
- 9) 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)
- 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.