COMING HOME

Ending Homelessness
in Middlesex County

Coming Home of Middlesex County, Inc.

Middlesex County Homeless Management Information System (MC HMIS) Policies and Procedures

1. Introduction

The countywide implementation of a Homeless Management Information System (HMIS) is administered by Coming Home of Middlesex County, Inc. (Coming Home or CHM) and WellSky Corporation (WellSky). WellSky administers the central server and CHM administers user and agency licensing, training and compliance. MC HMIS is an internet-based database that is used by homeless service organizations across Middlesex County to record and store Client-level information about the numbers, characteristics and needs of homeless persons and those at risk of homelessness.

MC HMIS enables service providers to measure the effectiveness of their interventions and facilitate longitudinal analysis of service needs and gaps within the Continuum of Care (CoC). Information that is gathered from consumers via interviews conducted by service providers is analyzed for an unduplicated count, aggregated (void of any identifying Client level information) and made available to policy makers, service providers, advocates, and consumer representatives. Data aggregated from MC HMIS about the extent and nature of homelessness in the Middlesex County is used to inform public policy decisions aimed at addressing and ending homelessness at local, State and federal levels.

Guidance for the implementation of Middlesex County's HMIS is provided by the CoC Executive Committee that is committed to understanding the gaps in services to consumers of the human service delivery system in an attempt to end homelessness. Implementation will be further guided by the MC HMIS Policy Review Committee, with direct feedback from MC HMIS end users.

This document provides the policies, procedures, guidelines and standards that govern MC HMIS operations, as well as the responsibilities for WellSky, the CoC Executive Committee, CHM and staff of agencies participating in MC HMIS (Partner Agency).

1.1 HMIS BENEFITS

Use of HMIS provides numerous benefits for service providers, homeless persons and Middlesex County.

Benefits for service providers:

- Provides online real-time information about Client needs and the services available for homeless persons.
- Assures confidentiality by providing information in a secured system.
- Decreases duplicative Client intakes and assessments.
- Tracks Client outcomes and provides a Client history.
- Generates data reports for local use and for state and federal reporting requirements.
- Facilitates the coordination of services within an organization and with other agencies and programs.
- Provides access to a statewide database of service providers, allowing agency staff to easily select a referral agency.

Benefits for homeless persons

- Intake information and needs assessments are maintained historically, reducing the number of times homeless persons must repeat their stories to multiple service providers.

- The opportunity to provide intake and life history one time demonstrates that service providers consider the homeless person's time to be valuable and restores some of the consumer's dignity.
- Multiple services can be easily coordinated and referrals streamlined

Benefits for Middlesex County

- Better able to define and understand the extent of homelessness throughout Middlesex County.
- Better able to focus staff and financial resources to the agencies and programs in geographical areas where services for homeless persons are needed the most.
- Better able to evaluate the effectiveness of specific interventions and specific programs and services provided.
- Better able to provide the County, State, and the federal government with data and information on the homeless population in Middlesex County.
- Better able to meet all local, State, and federal reporting requirements.

2. Requirements for Participation

2.1 HMIS ROLES AND RESPONSIBILITIES

CoC Executive Committee

1. Implement and continuously improve Middlesex County's HMIS.
2. Ensure the HMIS scope aligns with the requirements of agencies, HUD and other stakeholder groups.
3. Address any issue that has major implications for the HMIS, such as policy mandates from HUD or performance problems with the HMIS vendor.
4. Reconcile differences in opinions and approaches, and resolve disputes arising from them.
5. Review, revise and approve HMIS policies developed by the System Administrator.
6. With Coming Home, develop and approve the HMIS Policies and Procedures as the governance charter.

Software Vendor (*WellSky*)

1. Design the HMIS to meet HUD HMIS Data Standards.
2. Develop a codebook and provide other documentation of programs created.
3. Provide ongoing support to the HMIS System Administrator pertaining to needs of end-users to mine the database, generate reports and other end-user interface needs.
4. Administer the product servers including web and database servers.
5. Monitor access to HMIS through auditing.
6. Monitor functionality, speed and database backup procedures.
7. Provide backup and recovery of internal and external networks.
8. Maintain the system twenty-four hours a day, seven days a week.
9. Communicate any planned or unplanned interruption of service to the System Administrator.

System Administrator (*Coming Home of Middlesex County, Inc.*)

1. Monitor compliance with these Policies and Procedures and periodically review HMIS usage.
2. Communicate with participating organization leadership and other stakeholders regarding HMIS.
3. Authorize usage and access to HMIS for users who need access to the system for technical administration, data entry, editing of Client records, viewing of Client records, report writing, or administration of essential activities associated with carrying out HMIS responsibilities.
4. Develop reports.

5. Mine the database to respond to the information needs of participating organizations, community stakeholders and consumers.
6. Document work on the database and the development of reports/queries.
7. Provide technical assistance as needed with program sites.
8. Provide training and technical assistance to participating organizations on policies and procedures and system use, directly or through a consultant.
9. Respond to questions from users.
10. Coordinate technical support for system software.
11. Communicate with participants' problems with data entry and support data quality.
12. Monitor agency participation including timeliness and completeness of entry.
13. Communicate any planned or unplanned interruption in service.
14. Serve, in conjunction with Middlesex County, as the applicant to HUD for any HMIS grants that will cover the Continuum of Care geographic area.
15. Complete an annual security review.
16. Assess HMIS capacity and make recommendations to each agency on how to improve their technology as it relates to HMIS.
17. Assess current agency reporting needs, and developing plans for improved performance for programs currently entering data into HMIS.
18. Expand the use of HMIS to programs that currently are not tracking their data in HMIS.

Agency Administrator

1. Edit and update agency information in HMIS.
2. Ensure that the Partner Agency obtains a unique user license for each user at the agency.
3. Establish the standard report for each specific program created.
4. Ensure a minimum standard of data quality by answering all the HUD Universal Data Elements for every individual entered into HMIS by the agency.
5. Maintain the HUD required elements for each program.
6. Train new staff persons on HMIS, including reviewing the policies and procedures and any agency policies which impact the security and integrity of Client information.
7. Ensure that HMIS access is granted only to staff members that have received training and are authorized to use HMIS.
8. Grant technical access to HMIS for persons authorized by the System Administrator by creating usernames and passwords.
9. Notify all users at their agency of interruptions in service.
10. Provide a single point of communication between users and Coming Home.
11. Administer and monitor data security policies and standards, including:
    - User access control
    - The back- up and recovery of data
    - Detecting and responding to violations of the policies and procedures or agency policies

Users

1. Take appropriate measures to prevent unauthorized data disclosure.
2. Report any security violations.
3. Comply with relevant policies and procedures.
4. Input required data fields in a current and timely manner.
5. Inform Clients about the agency's use of HMIS.
6. Take responsibility for any actions undertaken with their usernames and passwords.

2.2 AGENCY ADMINISTRATION REQUIREMENTS

Participation Agreement Documents
Partner Agencies must complete the following documents:

1. **Coming Home Participating Agreement** must be signed by each Partner Agency's Executive Director. Coming Home will retain the original document. The Agreement includes the agency's commitment to adhere to the policies and procedures for effective use of MC HMIS.
2. **End User Agreement Document,** the form of which is an Exhibit to the Participation Agreement, must be signed by each authorized user .

User Access to the System
The Agency Administrator of the Partner Agency will determine user access for Case Managers and support staff to the specific program data within the Agency. The Agency Administrator will generate username and passwords within the administrative function of the software.

The Agency Administrator and all users must receive training before access to the system is granted.

Users who are also Clients Listed in HMIS
In order to prevent users from editing their own file or files of immediate family members, all users will agree to a conflict of interest statement. Users must disclose any potential conflict of interest to their Agency Administrator. Users will be prohibited from making changes to the information in their own file or the files of their immediate family members. If a user is suspected of violating this agreement, the System Administrator will run the audit trail report to determine if there was an infraction.

Passwords

- Creation: Passwords are automatically generated from the system when a user is created. The Agency Administrator will communicate the system-generated password to the user.
- Use: The user will be required to change the password the first time they log onto the system. The password must be at least 8 characters and alphanumeric. Passwords are the individual's responsibility and users cannot share passwords. Users may not keep written copies of their password in a publicly accessible location.
- Storage: Any passwords that are written down are to be stored securely and must be inaccessible to other persons. Users are not to store passwords on a personal computer for easier log on.
- Expiration: Passwords expire every 45 days. Users may not use the same password consecutively. Passwords cannot be re-used until 2 password selections have expired.
- Unsuccessful logon: If a user unsuccessfully attempts to log-on 3 times, the User ID will be "locked out," and access permission will be revoked rendering the user unable to gain access until his/her password is reset in the manner stated above.

Inputting Data
Agencies participating in the HMIS must meet the minimum data entry requirements established by the HUD Data & Technical Standards (see Attachment A).

Tracking of Unauthorized Access
Any suspicion of unauthorized activity should be reported to the System Administrator for MC HMIS.

Agency Administrator
Partner Agencies must designate one person to be the Agency Administrator.

The Agency Administrator will be responsible for creating usernames and passwords, and monitoring MC HMIS access by users at their agency. This person will also be responsible for training new agency staff persons on how to use HMIS.

The Agency Administrator must identify the assessments and requirements for each program, and properly set up each program in HMIS.

Client Consent

Partner Agencies are required to post in an area accessible to Clients that explains the electronic sharing of their personal information with other agencies that participate in HMIS when data sharing is appropriate for Client service.

Data Protocols

Partner Agencies must identify which data elements they wish to collect in addition to the minimally required data elements established in accordance with HUD's Data & Technical Standards.

2.3 POLICY REVIEW COMMITTEE REQUIREMENTS

Coming Home will convene and facilitate the MC HMIS Policy Review or Data Committee. CHM will invite members to serve on the Committee, and has the final authority to approve the appointment of any new member. All committee members must be active HMIS users.

CHM will make a proactive effort to have representation from consumer representatives, shelter and transitional housing programs, other homeless services organizations and government agencies that fund homeless assistance services. Replacement representatives will be invited to serve on the committee when participation from the organizations currently on the committee has been inconsistent or members are inactive.

Representation

Representation on the committee should take into consideration the following attributes:

- **User level** (e.g. Case Manager, Agency Administrator)
- **Size** or volume of the committee member's agency or program (e.g. Large or smaller)
- **Type** of service or program provided by the committee member's agency (e.g. Food Pantry or Transitional Housing)
- **Special interest** or demographic served by the committee member's agency (AIDS and DV)

Attendance

Policy Review/Data Committee members are required to attend all meetings. Members who are absent from two consecutive meetings must resign from the committee, unless there are extenuating circumstances.

Accessibility

The committee members will be visible and available for contact from HMIS users and agencies throughout the County.

Policies and Procedures

Approval of strategy, policy and procedures will be attempted through consensus and conversation, but will ultimately be decided by simple majority.

Letters of Commitment

All members of the Policy Review/Data Committee must sign letters of commitment.

Meeting Frequency

Meetings will be held quarterly. Important policy items that emerge in between meetings will be handled by the committee via e-mail.

2.4 HMIS USER LEVELS

Resource Specialist I

Users at this level may access only the ResourcePoint module. Users may search the database of area agencies and programs, and view the agency or program detail screens. A Resource Specialist I cannot modify or delete data, and does not have access to Client or service records or other modules and screens.

Resource Specialist II

Users may access only the ResourcePoint module. Users may search the database of area agencies and programs, and view the agency or program detail screens. At this level, the user does not have access to Client or service records or other modules and screens. A Resource Specialist II is an agency-level "Information & Referral (I&R) specialist" who may update their own agency and program information.

Resource Specialist III

Users at this level may access only the ResourcePoint module. Users may search the database of area agencies and programs and view the agency or program detail screens. A Resource Specialist III may add or remove resource groups, including Global (which they get by default). Access to Client or service records and other modules and screens is not given. A Resource Specialist III may edit the system-wide news feature.

Volunteer

Users may access ResourcePoint, and have limited access to ClientPoint and service records. A volunteer may view or edit basic demographic information about Clients (the profile screen), but is restricted from all other screens in ClientPoint. A volunteer may also enter new Clients, make referrals, and check-in/out Clients from a shelter. A volunteer does not have access to the "Services Provided" tab. This access level is designed to allow a volunteer to perform basic intake steps with a new Client and then refer the Client to an agency staff member or case manager.

Agency Staff

Users may access ResourcePoint, have full access to service records, and limited access to ClientPoint. Agency staff may access most functions in ServicePoint, however, they may only access basic demographic data on Clients (profile screen). All other screens are restricted including Reports. Agency Staff can add news items to the newswire feature.

Case Manager I

Users may access all screens and modules except "Administration." A Case Manager I may access all screens within ClientPoint, except the medical screen for confidentiality reasons. Users may access Reports.

Case Manager II

Users may access all screens and modules except "Administration." A Case Manager II may access all screens within ClientPoint, including the medical screen. Users may access Reports.

Table 1: HMIS User Roles

	Resource Specialist I	Resource Specialist II	Resource Specialist III	Volunteer	Agency Staff	Case Managers I & II	Case Manager III	Agency Administrator	Executive Director	System Operators	System Administrator I	System Administrator II
Client Point												
Profile				X	X	X	X	X	X		X	X
Assessments						X	X	X	X		X	X
Case Notes						X	X	X	X		X	X
Case Plans						X	X	X	X		X	X
Service Records				X	X	X	X	X	X		X	X
Service Point												
Referrals				X	X	X	X	X	X		X	X
Services Provided					X	X	X	X	X		X	X
Resource Point	X	X	X	X	X	X	X	X	X	X	X	X
Shelter Point				X	X	X	X	X	X		X	X
Administration												
Add/Edit Users								X	X	X	X	X
Reset Passwords								X	X	X	X	X
Add Provider			X							X	X	X
Edit Provider		#	X					#	#			
Delete Provider		%	X					%	%			
Agency News		X	X		X	X	X	X	X	X	X	X
System Wide News			X							X	X	X
Provider Groups												X
Picklist Data										X	X	X
Licenses										X	X	X
Assessment Admin										X	X	X
Shadow Mode												X
System Preferences												X

X: Users have access to this section of ServicePoint.

%: Users can neither delete the provider to which they belong, nor any of their parent providers.

#: Users cannot edit their parent provider; they may only edit their provider or child providers.

Case Manager III

This role has the same actions available as the Case Manager II with the added ability to see data down their provider's tree like an Agency Administrator.

Agency Administrator

Users may access all ServicePoint screens and modules. Agency Administrators may add/remove users and edit agency and program data for their agencies.

Executive Director

Users have the same access rights as Agency Administrator, but ranks above the Agency Administrator.

System Operator

Users may only access Administration screens. System operators can setup new agencies, add new users, reset passwords, and access other system-level options. Users may order additional user licenses and modify the allocation of licenses. They maintain the system, but may not access any Client or service records.

System Administrator I

Users have the same access rights to Client information as Agency Administrators, but for all agencies in the system. System Administrators also have full access to administrative functions.

System Administrator II

There are no system restrictions on users. They have full HMIS access.

2.5 HMIS VENDOR REQUIREMENTS

Physical Security

Access to areas containing HMIS equipment, data and software will be secured.

Firewall Protection

The vendor will secure the perimeter of its network using technology from firewall vendors. Company system administrators monitor firewall logs to determine unusual patterns and possible system vulnerabilities.

User Authentication

Users may only access HMIS with a valid username and password combination that is encrypted via SSL for internet transmission to prevent theft. If a user enters an invalid password three consecutive times, they are automatically shut out of that HMIS session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Application Security

HMIS users will be assigned a system access level that restricts their access to appropriate data.

Database Security

Wherever possible, all database access is controlled at the operating system and database connection level for additional security. Access to production databases is limited to a minimal number of points; as with production servers, production databases do not share a master password database.

Technical Support

The vendor will assist CH to resolve software problems, make necessary modifications for special programming, and will explain system functionality to CH.

Technical Performance
The vendor maintains the system, including data backup, data retrieval and server functionality/operation. Upgrades to the system software will be continuously developed and implemented.

Hardware Disposal
Data stored on broken equipment or equipment intended for disposal will be destroyed using industry standard procedures.

2.6 MINIMUM TECHNICAL STANDARDS

Minimum Workstation Requirements
Memory
- If Win10 – 4 Gig recommended, (2 Gig minimum)

Monitor
- Screen Display - 1024 by 768 (XGA) or higher (1280x768 strongly advised)

Processor
- A Dual-Core processor is recommended.
- Avoid using a single-core CPUs.

Internet Connection
- Broadband

Browser
- Chrome is recommended
- Firefox is a good alternate
- Microsoft Edge are acceptable.

Recommended Practices
- Microsoft Windows: Update as patches become available.
- Browser: Update as patches become available.
- Workstation Maintenance: Provide regularly scheduled maintenance on all workstations.

Although there is no unusual hardware or additional ServicePoint-related software required to connect to the database, the speed and quality of the Internet connection and the speed of the hardware and could have a profound affect on the ease of data entry and report extraction. A high-speed Internet connection, like a DSL or ISDN line with speeds at or above 128.8 Kbps, is preferred, as is a computer with speeds above 166MHz. WellSky also recommends the use of Windows 2000 or XP (1 GHz models or faster) as the Windows platform to eliminate certain technical problems.

2.8 HMIS LICENSE FEES

Annual MC HMIS License Fees
Agencies may purchase licenses at any time. License fees are set forth in the User Participating Agreement. License fee arrangements are subject to change by Coming Home in consultation with the MC HMIS policy/Data committee. Additional licenses may be purchased as needed, for an additional fee. Billing for licenses will occur once annually to be paid within 60 days following receipt of the invoice.

3. **Privacy**

The importance of the integrity and security of MC HMIS cannot be overstated. Given this importance, HMIS must be administered and operated under high standards of data quality and security. Coming Home and Partner Agencies are jointly responsible for ensuring that HMIS data processing capabilities, including the collection, maintenance, use, disclosure, transmission and destruction of data, comply with the MC HMIS privacy, security and confidentiality policies and procedures. When a privacy or security standard conflicts with other Federal, State and local laws to which the partner agency must adhere, the partner agency must contact Coming Home to collaboratively update the applicable policies for the Partner Agency to accurately reflect the additional protections.

3.1 DATA SHARING AND ACCESS

All MC HMIS data will be handled according to the following major classifications: Shared or Closed Data. CHM will assess all data, and implement appropriate controls to ensure that data classified as shared or closed is handled according to the following procedures.

3.1.1 Definitions

Shared Data
Shared data is unrestricted information that has been entered by one provider and is visible to other providers using HMIS. Middlesex County's HMIS is designed as an open system that defaults to allow shared data.

Closed Data
Information entered by one provider that is not visible to other providers using MC HMIS. The System Administrator will establish the visibility settings for certain information as closed (e.g. HIV/AIDS status). Individual Client records can be closed by the provider at the Client's request.

De-identified Data
Data that has specific Client demographic information removed, allowing use of the data ***without identifying*** a specific Client; also referred to as "non-identifying" information.

Identified Data
Data that can be used to identify a specific Client; also referred to as "Confidential" data or information.

Procedures for transmission and storage of data

- De-identified Data: May be discussed and released without a Client's consent.
- Identified Data: Each Partner Agency shall develop rules governing the access of identified data in MC HMIS to ensure that those staff needing such access will have access, and access is otherwise restricted. The agency rules shall also cover the destruction of paper and electronic data in a manner that will ensure that privacy is maintained and that proper controls are in place for any hard copy and electronic data that is based on MC HMIS data.

Whenever identified data is accessed:

- Hard copies shall be shredded when disposal is appropriate. Hard copies shall be stored in a secure environment that is inaccessible to the general public or staff not requiring access.
- Hard copies shall not be left out in the open or unattended.
- Electronic copies shall be stored only where the employee can access the data.
- Electronic copies shall be stored where a password is required to access the data if on shared server space.

3.2 DATA REPORTING PARAMETERES AND GUIDELINES

3.2.1 Definitions

Public Data
Any data that is included in any form, application, report, or any other submission to a public entity.

Principles for Release of Data

- Only de-identified aggregated data will be released except as specified below.
- No Identified Data may be released without informed consent unless otherwise specified by State and federal confidentiality laws. All requests for such information must be addressed to the owner/participating agency where the data was collected.
- Once deemed Public, data can be released without security controls.
- There will be full access to aggregate data included in published reports.
- Reports of aggregate data may be made directly available to the public.
- The parameters of the aggregated data, that is, where the data comes from and what it includes will be presented with each report.
- Data will be mined for agencies requesting reports on a case-by-case basis.
- Requests must be written with a description of specific data to be included and for what duration of time. Requests are to be submitted 30 days prior to the date the report is needed. Exceptions to the 30-day notice may be made.
- CHM reserves the right to deny any request for aggregated data.

3.3 RELEASE OF DATA FOR GRANT FUNDERS

Entities providing funding to agencies or programs required to use HMIS will not have automatic access to HMIS. Access to HMIS will only be granted by CH when there is a voluntary written agreement in place between the funding entity and the agency or program.

3.4 BASELINE PRIVACY POLICY

Collection of Personal Information
Personal information will be collected for HMIS only when it is needed to provide services, when it is needed for another specific purpose of the agency where a Client is receiving services, or when it is required by law. Personal information may be collected for these purposes:

- To provide or coordinate services for Clients.
- To find programs that may provide additional Client assistance.
- To comply with government and grant reporting obligations.
- To assess the state of homelessness in the community, and to assess the condition and availability of affordable housing to better target services and resources.

Only lawful and fair means are used to collect personal information.

Personal information is collected with the knowledge and consent of Clients. It is assumed that Clients consent to the collection of their personal information as described in this notice when they seek assistance from an agency using HMIS and provide the agency with their personal information.

If an agency reasonably believes that a Client is a victim of abuse, neglect or domestic violence, or if a

Client reports that he/she is a victim of abuse, neglect or domestic violence, explicit permission is required to enter and share the Client's information in HMIS.

Your personal information may also be collected from:

- Additional individuals seeking services with a Client.
- Other private organizations that provide services and participate in HMIS.

Clients must be able to access the Use and Disclosure of Personal Information policy found below.

Use and Disclosure of Personal Information

These policies explain why an agency collects personal information from Clients. Personal information may be used or disclosed for activities described in this part of the Policy. Client consent to the use or disclosure of personal information for the purposes described in this section, and for reasons that are compatible with purposes described in this section but not listed, is assumed. Clients must give consent before their personal information is used or disclosed for any purpose not described here.

Personal information may be used or disclosed for the following purposes:

- To provide or coordinate services to individuals. Client records are shared with other organizations that may have separate privacy policies and that may allow different uses and disclosures of the information. If Clients access services at one of these other organizations, they will be notified of the agency's privacy and sharing policy.
- To carry out administrative functions such as legal audits, personnel, oversight, and management functions.
- For research and statistical purposes. Personal information released for research and statistical purposes will be anonymous.
- For academic research conducted by an individual or institution that has a formal relationship with Middlesex County and/or Coming Home. The research must be conducted by an individual employed by or affiliated with the organization or institution. All research projects must be conducted under a written research agreement approved in writing by the designated agency administrator or executive director. The written research agreement must:
  1. Establish the rules and limitations for processing personal information and providing security for personal information in the course of the research.
  2. Provide for the return or proper disposal of all personal information at the conclusion of the research.
  3. Restrict additional use or disclosure of personal information, except where required by law.
  4. Require that the recipient of the personal information formally agree to comply with all terms and conditions of the written research agreement, and
  5. Cannot be a substitute for approval of the research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution if appropriate.

- When required by law, Identified Information will be released to the extent that use or disclosure complies with the requirements of the law.
- To avert a serious threat to health or safety if:
  1. 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.
- To report to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence, information about an individual reasonably believed to be a victim of abuse, neglect or domestic violence. When the

personal information of a victim of abuse, neglect or domestic violence is disclosed, the individual who's information has been released will promptly be informed, except if:
  1. it is believed that informing the individual would place the individual at risk of serious harm, or
  2. a personal representative (such as a family member or friend) who is responsible for the abuse, neglect or other injury is the individual who would be informed, and it is believed that informing the personal representative would not be in the best interest of the individual as determined in the exercise of professional judgment.
- For a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
  1. 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 court ordered disclosure goes through the State.
  2. If the law enforcement official makes a written request for personal information. The written request must meet the following requirements:
     - i. Is signed by a supervisory official of the law enforcement agency seeking the personal information.
     - ii. States that the information is relevant and material to a legitimate law enforcement investigation.
     - iii. Identifies the personal information sought.
     - iv. Is specific and limited in scope to the purpose for which the information is sought, and
     - v. Is approved for release by the State legal counsel after a review period of seven to fourteen days.
  3. If it is believed that the personal information constitutes evidence of criminal conduct that occurred at the agency where the Client receives services.
  4. If the official is an authorized federal official seeking personal information for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to a foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 (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.
- For law enforcement or another public official authorized to receive a Client's Identified Information, to conduct an immediate enforcement activity that depends upon the disclosure. Identified Information may be disclosed when a Client is incapacitated and unable to agree to the disclosure if waiting until the individual is able to agree to the disclosure would materially and adversely affect the enforcement activity. In this case, the disclosure will only be made if it is not intended to be used against the individual.
- To comply with government reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.

<u>Inspection and Correction of Personal Information</u>

Clients may inspect and receive a copy of their personal information maintained in MC HMIS. The agency where the Client receives services will offer to explain any information that a Client may not understand.

If the information listed in MC HMIS is believed to be inaccurate or incomplete, a Client may submit a verbal or written request to have his/her information corrected. Inaccurate or incomplete data may be deleted, or marked as inaccurate or incomplete and supplemented with additional information.

A request to inspect or copy one's personal information may be denied if:

- The information was compiled in reasonable anticipation of litigation or comparable proceedings
- The information was obtained under a promise or confidentiality and if the disclosure would reveal the source of the information, or
- The life or physical safety of any individual would be reasonably endangered by disclosure of the personal information.

If a request for inspection access or personal information correction is denied, the agency where the Client receives services will explain the reason for the denial. The Client's request and the reason for the denial will be included in the Client's record.

Requests for inspection access or personal information correction may be denied if they are made in a repeated and/or harassing manner.

Data Quality

Only personal information relevant for the purpose(s) for which it will be used will be collected. Personal information must be accurate and complete.

Client files not used in seven years may be made inactive in MC HMIS. CH will check with agencies before making Client files inactive. Personal information may be retained for a longer period if required by statute, regulation, contract or another obligation.

Complaints and Accountability

Questions or complaints about the privacy and security policies and practices may be submitted to the agency where the Client receives services. Complaints specific to HMIS should be submitted to the Agency Administrator and program director. If no resolution can be found, the complaint will be forwarded to the System Administrator (Coming Home) and the Agency's Executive Director. If there is no resolution, the MC HMIS Policy/Data Committee will oversee final arbitration. All other complaints will follow the agency's grievance procedure as outlined in the agency's handbook.

All MC HMIS users (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy notice. Users must receive and acknowledge receipt of a copy of this privacy notice.

3.5 USE OF A COMPARABLE DATABASE BY VICTIM SERVICE PROVIDERS

Victim service providers, private nonprofit agencies whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking, must not directly enter or provide data into HMIS if they are legally prohibited from participating in HMIS. Victim service providers that are recipients of funds requiring participation in HMIS, but are prohibited from entering data in HMIS, must use a comparable database to enter Client information. A comparable database is a database that can be used to collect Client-level data over time and generate unduplicated aggregated reports based on the Client information entered into the database. The reports generated by a comparable database must be accurate and provide the same information as the reports generated by HMIS.

3.6 USER CONFLICT OF INTEREST

Users who are also clients with files in MC HMIS are prohibited from entering or editing information in their own file. All users are also prohibited from entering or editing information in files of immediate family members. All licensed End Users agree to this limitation and to report any potential conflict of interest to their Agency Administrator. The System Administrator may run the audit trail report to determine if there has been a violation of the conflict of interest agreement.

4. **Security**

4.1 USER SECURITY

Agency Administrators will provide unique user names and initial passwords to each Partner Agency user. User names will be unique for each user and will not be exchanged or shared with other users. The MC HMIS System Administrator will have access to the list of user names for the MC HMIS and will track user name distribution and use. Only CH will be authorized to purchase or grant additional user licenses to an Agency that has utilized all current licenses.

Agency Administrators will provide unique user names and initial passwords to each user upon completion of training and MC HMIS Policies and Procedures. The sharing of user names will be considered a breach of these policies. Agency Administrators are responsible for distributing user names and initial passwords to agency users as well as for providing current users with a new password if he/she requires one.

4.2 USER CHANGES

The Partner Agency Administrator will make any necessary changes to the Partner Agency user accounts. This includes issuance of new passwords, revoking authorization for staff that is no longer with the agency, and managing access levels, etc. The Agency Administrator has the ability to change user names and redistribute user licenses to accommodate the Partner Agency organization.

Changes in Agency Administrators must be reported to the MC HMIS System Administrator. The Agency Administrator is required to revoke the user license of a terminated employee immediately upon termination of employment. For employees with user access otherwise leaving the agency, the user license should be revoked at the end of business on the person's last day of employment.

4.3 PASSWORDS

Users will have access to the MC HMIS via a user name and password. Passwords must be changed a minimum of once every 45 days. Users will keep passwords confidential. Under no circumstances shall a licensed user share a password nor shall they post their password in an unsecured location. These methods of access are unique to each user and confidential. Users are responsible for keeping their passwords confidential.

The Agency Administrator will issue a user name and temporary password to each new user who has completed training. Upon sign in with the user name and temporary password, the user will be required by the software to select a unique password that will be known only to him/her. Every 45 days, passwords are reset automatically by the MC HMIS software. See Section B.1 for additional detail on password security.

4.4 PASSWORD RECOVERY

The Agency Administrator will reset a user's password in the event the password is lost or forgotten. The Agency Administrator will reset the user password, and issue a temporary password to allow the user to login and choose a new password. The new password will be valid from that time forward, until the next 45-day forced change. Agency Administrators must validate the authenticity of the request if the request is not made in person. In other words, neither Agency Administrators nor the MC HMIS System Administrator shall issue a new password without ensuring that the person requesting it is, in fact, the person with the authorization to use it.

4.5 EXTRACTED DATA

MC HMIS users will maintain the security of any Client data extracted from the database and stored locally, including all data used in custom reporting. MC HMIS users will not electronically transmit any unencrypted Client data across a public network.

The custom report-writer function of ServicePoint allows Client data to be downloaded to an encrypted file on the local computer. Once that file is unencrypted by the user, confidential Client data is left vulnerable on the local computer, unless additional measures are taken. Such measures include restricting access to the file by adding password. For security reasons, unencrypted data may not be sent over a network that is open to the public. Unencrypted data may not be sent via email. HMIS users should apply the same standards of security to local files containing Client data as to the HMIS database itself. Data extracted from the database and stored locally will be stored in a secure location (not on floppy disks/CDs or other temporary storage mechanisms like flash drives or on unprotected laptop computers, for example) and will not be transmitted outside of the private local area network unless it is properly protected via encryption or by adding a file-level password. The MC HMIS System Administrator will provide help in determining the appropriate handling of electronic files. All security questions will be addressed to the MC HMIS System Administrator. Breach of this security policy will be considered a violation of the user agreement, which may result in personnel action and/or agency sanctions.

4.6 DATA ACCESS COMPUTER REQUIREMENTS

Users will ensure the confidentiality of Client data, following all security policies in the MC HMIS Policies and Procedures and adhering to the standards of ethical data use, regardless of the location of the connecting computer. All Policies and Procedures and security standards will be enforced regardless of the location of the connecting computer.

Because ServicePoint is web-enabled software, users could conceivably connect to the database from locations other than the Partner Agency itself, using computers other than agency-owned computers. Connecting from a non-agency location may introduce additional threats to data security, such as the ability for non- ServicePoint users to view Client data on the computer screen or the introduction of a virus. If such a connection is made, the highest levels of security must be applied, and Client confidentiality must still be maintained. This includes only accessing the MC HMIS via a computer that has virus protection software installed and updated

Each Partner Agency and Agency Administrator is responsible for:

- Physical Space: Partner Agencies must take reasonable steps to ensure Client confidentiality when licensed users are accessing the MC HMIS. Licensed users are required to conduct data entry in a protected physical space to prevent unauthorized access to the computer monitor while confidential Client information is accessible.
- Use of a non-agency computer located in a public space (i.e. internet café, public library) to connect to HMIS is prohibited.
- Time-Out Routines: Each Agency Administrator will be required to enable time-out (login/logout) routines on every computer to shut down access to the MC HMIS when a computer is unattended. Time-out routines will be engaged at a minimum after 10 minutes of inactivity or at other intervals as CHM determines.
- Each computer that accesses MC HMIS must have current virus software that updates automatically installed.
- If the MC HMIS is accessed over a network, the network must be protected by a hardware or

software Firewall at the Server. A stand-alone machine that accesses HMIS must also have a hardware or software Firewall installed and active. This may be the Firewall protection included as part of the operating system or the virus protection software installed on the computer.

4.7 SECURITY PROCEDURE TRAINING FOR USERS

All users must receive security training prior to being given access to MC HMIS. Security training will be covered during the new user training for all new users. All users must receive on-going annual training on security procedures from their Agency Administrators and/or Coming Home.

4.8 VIOLATION OF SECURITY PROCEDURES

All potential violations of any security protocols will be investigated and any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to: a formal letter of reprimand, suspension of system privileges, revocation of system privileges and criminal prosecution.

If possible, all confirmed security violations will be communicated in writing to the affected Client within 14 days, unless the Client cannot be located. If the Client cannot be located, a written description of the violation and efforts to locate the Client will be prepared by CHM and placed in the Client's file at the Agency that originated the Client's record.

Any agency that is found to have consistently and/or flagrantly violated security procedures may have their access privileges suspended or revoked. All sanctions are imposed by Coming Home. All sanctions may be appealed to Coming Home's Executive Director.

4.9 PROCEDURE FOR REPORTING SECURITY INCIDENTS

Users and Agency Administrators should report all unlawful access of MC HMIS and unlawful attempted access of HMIS. This includes theft of usernames and passwords. Security incidents should be reported to the System Administrator. The System Administrator will use the HMIS user audit trail report to determine the extent of the breach of security.

4.10 DISASTER RECOVERY PLAN

Middlesex County's HMIS is covered under WellSky's Disaster Recovery Plan. Due to the nature of technology, unforeseen service outages may occur. In order to assure service reliability, WellSky provides the following disaster recovery plan. Plan highlights include:

- Database tape backups occur nightly.
- Tape backups are stored offsite.
- Seven day backup history is stored locally on instantly accessible Raid 10 storage.
- One month backup history is stored off site.
- Access to WellSky's emergency line to provide assistance related to "outages" or "downtime" 24 hours a day.
- Data is backed up locally on instantly-accessible disk storage every 24 hours.
- The application server is backed up offsite, out-of-state, on a different internet provider and on a separate electrical grid via secured Virtual Private Network (VPN) connection.
- Backups of the application site are near-instantaneous (no files older than 5 minutes).
- The database is replicated nightly at an offsite location in case of a primary data center failure.
- Priority level response (ensures downtime will not exceed 4 hours).

Standard Data Recovery

Middlesex County's HMIS database is stored online, and is readily accessible for approximately 24 hours a day. Tape backups of the database are kept for approximately one month. Upon recognition of a system failure, MC HMIS can be copied to a standby server. The database can be restored, and the site recreated within three to four hours if online backups are accessible. As a rule, a tape restoration can be made within six to eight hours. On-site backups are made once daily. A restore of this backup may incur some data loss between when the backup was made and when the system failure occurred.

All internal servers are configured in hot-swappable hard drive RAID configurations. All systems are configured with hot-swappable redundant power supply units. Our Internet connectivity is comprised of a primary and secondary connection with separate internet service providers to ensure redundancy in the event of an ISP connectivity outage. The primary Core routers are configured with redundant power supplies, and are configured in tandem so that if one core router fails the secondary router will continue operation with little to no interruption in service. All servers, network devices, and related hardware are powered via APC Battery Backup units that are connected in turn to electrical circuits, which are connected to a building generator.

All Client data is backed-up online and stored on a central file server repository for 24 hours. Each night a tape backup is made of the Client database and secured in a bank vault.

Historical data can be restored from tape as long as the data requested is newer than 30 days old. As a rule, the data can be restored to a standby server within four hours without affecting the current live site. Data can then be selectively queried and/or restored to the live site.

For power outage, MC HMIS is backed up via APC battery back-up units, which are connected via generator-backed up electrical circuits. For a system crash, a system restore will take four hours. There is potential for some small data loss (data that was entered between the last backup and when the failure occurred) if a tape restore is necessary. If the failure is not hard drive related, the data restore time will possibly be shorter as the drives themselves can be repopulated into a standby server.

All major outages are immediately brought to the attention of executive management. WellSky Systems support staff helps manage communication or messaging to the System Administrator as progress is made to address the service outage.

5. Data Quality Requirements

5.1 DATA COLLECTION PROTOCOL

Partner Agencies are responsible for asking all Clients a minimum set of questions for use in aggregate analysis. These questions are included in custom assessments that are created by the System Administrator, in conjunction with the CoC, and meet the requirements set forth by HUD in the HUD Data & Technical Standards (see Attachment C). The required data elements depend on the program. The mandatory data elements in each assessment will require that an answer be entered before you can progress to the next data element.

Programs that do not adhere to the minimum data entry standards will be notified of their deficiencies and given appropriate training on how to correctly enter data. Programs that do not meet minimum data entry standards will have MC HMIS access suspended until such time that CH believes the program could begin to correctly enter information. After the two initial warnings from CH, a program still not adhering to the minimum data entry requirements will be made permanently inactive, and licenses will be revoked until the agency can demonstrate to CHM that it is capable of maintaining minimum data requirements.

CHM will submit a report to the CoC annually that identifies the degree to which each all agencies within the CoC are meeting the minimum data entry standards.

The Agency Administrator must identify the assessments and requirements for each program, and properly set up each program in MC HMIS.

5.2 DATA INTEGRITY AND RELIABILITY

Partner Agencies are responsible for the overall quality, accuracy and completeness of data entered by their staff for their Clients. CHM will monitor data collection for random variables and hold Partner Agencies accountable for not entering required data.

5.3 DATA OWNERSHIP

The MC HMIS, and any and all data stored in the MC HMIS, is the property of Coming Home. CHM has authority over the creation, maintenance, and security of the MC HMIS. Violations of the MC HMIS Agency Agreement, the Policies and Procedures, privacy policies developed at the agency level, or other applicable laws may subject the Partner Agency to discipline and/or termination of access to the MC HMIS and/or to termination of other contracts.

The Participating Agency Agreement includes terms regarding the maintenance of the confidentiality of Client information, provisions regarding the duration of access, an acknowledgement of receipt of the Policies and Procedures, and an agreement to abide by all policies and procedures related to the MC HMIS including all security provisions contained therein. Because programs participating in the MC HMIS are funded through different streams with different requirements (HUD, State, County, and other), CHM shall maintain ownership of the database in its entirety in order that these funders cannot access data to which they are not legally entitled.