NEW JERSEY HOMELESS MANAGEMENT INFORMATION SYSTEM
Policies & Procedures Manual

Table of Contents

Introduction

New Jersey's HMIS is a collaborative effort between the New Jersey Housing Mortgage Finance Agency (HMFA), the dedicated lead agency, and seventeen of New Jersey's Continuums of Care. The Continuums of Care, individually or as a group, have an ongoing role in giving input into HMIS policy decisions within the parameters established by the U.S. Department of Housing and Urban Development (HUD). The Continuums of Care retain the right to withhold support for HMIS.

New Jersey's HMIS project is governed by a HMIS Steering Committee, which will include representatives from NJ HMFA, New Jersey's Department of Community Affairs, and New Jersey's Department of Human Services.

A New Jersey HMIS Advisory Council will meet quarterly to review recommendations for system-wide changes in functionality and system-flow. The Advisory Council consists of a maximum of two representatives from each participating Continuum of Care, as well as representatives from NJ HMFA. All Continuum of Care representatives will participate in the Advisory Council on a voluntary basis, and representatives will be selected by their home CoC. The CoC's are responsible for communicating the identities of their Advisory Council representatives to NJ HMFA.

All organizations participate in the HMIS Advisory Council on a voluntary basis and select their own representatives. Organizations are responsible for communicating with NJ HMFA about the identity of their respective representatives.

The methods of communication between the System Administrator and the participating agencies will be via electronic mail or telephone.

This manual contains all of the most current operational policies and procedures related to New Jersey's Homeless Management Information System (NJHMIS). It is expected that Policies and Procedures will be removed, added, and modified as circumstances dictate. That is why this manual is designed to be modular. Because the *HMIS Policies and Procedures Manual* is contained in a loose-leaf notebook, outdated policies and procedures can easily be removed, and updated policies and procedures can easily be inserted.

For more information regarding NJHMIS Policies and Procedures, please contact Catherine Brewster, New Jersey Housing Mortgage Finance Agency, at 609-278-7567 or cbrewster@njmhfa.gov

Confidentiality, Privacy, and Security

HMIS Privacy & Security Standards
Federal Register – July 30, 2004

Section 4

- Based on principles of fair information practices & security standards recognized by the information privacy & technology communities
- Developed after careful review of the HIPPA standards
- Baseline standards required by any organization that records, uses or processes PPI on homeless clients for a HMIS.
- Additional protocols or policies to enhance further privacy & security for individual agencies, as deem appropriate
- Organizations must comply with federal, state and local laws re: confidentiality protections
- Two-tiered approach: minimum must meet the baseline privacy & security requirements/Some agencies may adopt higher levels of security due to nature of homeless population

Section 4.1.1 Definition of Terms

- Definitions:
  Protected Personal Information (PPI) – any information maintained about a living homeless client or individual that identifies/manipulated/linked to a specific individual
  Covered Homeless Organization (CHO)-any organization that records, uses or processes PPI on homeless clients for a HMIS
  Processing-any operation or set of operations performed on PPI for collection, maintenance, use, disclosure, transmission & destruction of information
  HMIS Uses and disclosures – uses and disclosures allowed by these standards

Section 4.1.2 Applying HMIS Privacy & Security Standards

- Any CHO covered under HIPAA, is not required to comply with privacy/security standards, if, a substantial portion of its PPI is protected health information as defined in HIPAA. (See Exemptions) HMIS standards give precedence to the HIPAA rules: 1) HIPAA rules more finely attuned to requirements of health care system; 2) important privacy & security protections; 3) unreasonable burden to follow two sets of rules
- IF PPI does not fall under standards in this section; must be described in privacy notice with explanation of reason not covered. Disclosure requirement necessary if other standards are being used other than the HMIS standards

Section 4.1.3 Allowable HMIS uses & disclosures of PPI

- Allowable uses: 1) provide or coordinate services; 2) services related to payment or reimbursement; 3) carry out administrative functions; 4) creating de-identified PPI
- Uses/disclosures required by law-must comply & be limited to the requirements of the law
- Uses and disclosures to avert a serious threat to health or safety
- Uses and disclosures about victims of abuse, neglect or domestic violence
    - Required by law and complies with and limited to requirements of law
    - If client agrees to disclosure
    - Authorized by statute or regulation; necessary to prevent serious harm or if individual is incapacitated and not intended to be used against individual
    - Must inform individual that a report has been made; See Exception

- Uses and disclosures for academic research; must be formal relationship-See section for further discussion
- Disclosures for law enforcement purposes; court order, warrant, subpoena or summons. **See section for further discussion**

Section 4.2 Privacy Requirements

- Must comply with baseline privacy requirements
    - Data collection limitations
    - Data quality
    - Purpose use limitations
    - Openness
    - Access & correction
    - Accountability
- May adopt additional substantive & procedural privacy protections that exceed baseline standards
- Comply with federal, state and local laws
- Must be described in privacy notice
- Maintain a common data storage medium with another organization for sharing of PPI; responsibility for privacy & security by both organizations; must comply with HMIS standards and allow for un-duplication of homeless clients at CoC level

Section 4.2.1 Collection Limitation

- Collection of PPI only when appropriate to the purposes for which information is obtained or required by law
- Collect by lawful and fair means with knowledge and consent of individual
- Post a sign at each intake desk, which explains reasons for collection
- Additional Privacy Protections – In Privacy Notice commit to additional privacy protections consistent with HMIS requirements; 1) restricting collection of PPI; 2) collection PPI only with express knowledge; 3) oral/written consent from individual/third party

Section 4.2.2 Data Quality

- PPI collected must be relevant to the purpose for which it is to be used
    - Accurate, complete and timely
- Develop & implement plan to dispose of or, remove identifiers seven (7) years after creation or last changed See **Section 4.3 for further discussion**

Section 4.2.3 Purpose Specification/Use Limitation

- Specify in Privacy notice purposes for collecting PPI and describe all uses and disclosures
- If not disclosed in Privacy notice must have consent of individual
- Additional Privacy Protections
    - Must be consistent with HMIS requirements
    - Seek oral/written consent for some or all processing
    - Agree to additional restrictions at request of individual
    - Limiting uses/disclosures as stated in privacy notice
    - No disclosure of PPI unless required by statute
    - Maintain audit trail containing date, purpose & recipient
    - Make audit trails available to homeless individual
    - Limit disclosure of PPI to minimum necessary for purpose

Section 4.2.4 Openness

- Publish Privacy Notice, describe policies & practices, provide copy upon request
- Current version on web page
- Must post sign stating availability of privacy notice
- Privacy notice must state may be amended at any time; amendments may affect information obtained prior to change, unless otherwise stated
- Amendments must adhere to HMIS privacy standards
- Must maintain permanent documentation of all amendments
- Provide accommodations for persons with disabilities throughout data collection process See **Section for further discussion**
- Provide required information in other languages other than English, common to community
- Additional Privacy protections-**See section for further discussion**

Section 4.2.5 Access and Correction

- Must allow client to inspect and obtain copy of any PPI about client
- Must offer explanation of any questions
- Must consider any request by client for correction of inaccurate or incomplete PPI pertaining to client
- A CHO is not required to remove PPI information, may mark information as inaccurate or incomplete and may make additions
- Privacy Notice may reserve the ability to deny client to inspect and obtain copy

    - Litigation or comparable proceedings
    - Information about another individual
    - Promise of confidentiality, if disclosure would reveal source of information
    - Information that would endanger the life or physical safety of individual
- Upon denial to inspect or obtain copy, CHO must explain reason for the denial, include request documentation as part of PPI
- Additional Privacy Protections-CHO may in its privacy notice, commit to additional privacy protections consistent with HMIS requirements
    - Adopt own appeal procedure and describe within privacy notice
    - Limit grounds for denial, by not stating specific basis for denial
    - Allow client to add disagreement to PPI and allow to share disputed information to another person
    - Provide written explanation of reason for denial

Section 4.2.6 Accountability

- Establish procedure for accepting/considering questions/complaints about privacy and security policies and practices
- A CHO must require all staff members to sign a confidentiality agreement acknowledging receipt of a copy of privacy notice and pledges to comply with privacy notice
- Additional Privacy Protections- 1) may request staff to undergo formal training in privacy requirements; 2) Establish method for regularly reviewing compliance with privacy notice; 3) Establish internal/external appeal process for appeal of privacy complaint; 4) Designate a chief privacy officer for implementation of privacy standards

Section 4.3 Security Standards

- All CHOs must comply with baseline security requirements

Section 4.3.1 System Security

- Must apply system security provisions to all systems where PPI is stored
    - System Networks
    - Desktops
    - Laptops
    - Mini-computers
    - Mainframes
    - Servers
- Additional Security Protections-1) apply system security provisions to electronic and hard copy information that is not collected for HMIS; 2) May seek outside collaboration for performing internal security audit and certify system security
- HMIS systems must have a user authentication system consisting of a username and a password; passwords must be at least eight characters long and meet reasonable industry standard requirements

    - At least one number and one letter
    - Not using the username, the HMIS name or the HMIS vendors name
    - Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards
    - Default passwords on initial entry, must be changed upon first use
    - Written user access may not be stored or displayed in public access area
    - Individual users must not have access to more than one workstation or long on to the network at more than one location at a time
    - Additional Security Protections- 1) upper and lower case letters; 2) numbers; 3) symbols
    - Complex passwords-Use phrases, not individual words; capitalize each new word; substitute numbers and symbols for letters; eliminate spaces between words
- CHOs must protect HMIS systems by using commercial virus protection software
- Must include automated scanning of files, as accessed by users
- Must regularly update virus definitions from software vendor
- May commit to automatically scanning all files for viruses when system turned on, shut down or not actively being used
- Must have secure firewall between workstation and any systems
- Modem access must have own firewall
- Central server access, server must have firewall
- Older operating systems may need to be equipped with secure firewalls
- Additional security protections-Apply firewall to all workstations
- Public Access-Public forums for data collection or reporting must be secured to allow connections from pre-approved computers and systems through Public Key Infrastructure (PKI) certificates; or extranets that limit access **See Section for further discussion**
- Physical Access to Systems with HMIS Data-Computers must be staffed at all times when located in public areas
- Steps to ensure that the computers and data is secured at all times
- Workstations should automatically turn on a password protected screensaver when workstation temporarily not in use; time for password protection can be regulated by CHO
- Staff should log off and shut down data entry system when gone for an extended period of time
- **See section on additional security protections**
- All HMIS data must be copied to another medium on a regular basis and store in a secure of-site location
- Central server must be stored in a secure room with appropriate temperature control and fire suppression systems
- Surge protectors must be used
- CHOs must reformat storage medium when deleting all HMIS data; reformat storage medium more than once before reusing or disposing the medium

- Appropriate methods in place to monitor security systems
- HMIS data must maintain a user access log; logs must be checked routinely

Section 4.3.2 Application Security

- Apply application security provisions to software during data entry, storage and review or any other processing function
- All HMIS data must be encrypted when electronically transmitted
- Current standard is 128-bit encryption
- **See section regarding unencrypted data**
- All HMIS data must be stored in a binary, not text, format
- All paper or other hard copy containing PPI for HMIS must be secured
    - Reports
    - Data entry forms
    - Signed consent forms
- All paper or other hard copy containing PPI must be supervised at all times when in public area

a. Protected Personal Information

Any information that can be used to identify a particular individual is protected personal information. HMIS users and developers must consider the following as protected personal information of an individual and his or her relatives, employers, or household members:

- Names
- All geographic subdivisions smaller that a state, including street address, city, county, precinct, zip code, and their equivalent geocodes.
- All elements of dates (except year) directly related to an individual, including birth date, admission date, discharge date, and date of death.
- Telephone numbers
- Social Security numbers
- Medical record numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Any other unique identifying number, characteristic, or code

b. <u>Unidentifiable Data</u>

Agency data will always be extracted and published at the non-identifiable level. The AWARDS ID will be used to link clients across agencies and, by linking clients at the non-identifiable level, will preserve client anonymity. In addition, the Common Index provides a method of developing unduplicated client counts across agencies.

- All client data retrieved for custom reports will be individual, yet non-identifiable data. (For example, a client name “Mary Smith” will never show up in a report as “Mary Smith,” but as “SD123FGH”.)

- All HMIS data that are electronically transmitted over publicly accessible networks or phone lines will have at least 128-bit encryption, which is the industry standard. Unencrypted data may be transmitted over secure direct connections. A secure direct connection is one that can only be accessed by users who have been authenticated on at least one of the systems involved and does not utilize any tertiary systems to transmit data.

- All HMIS protected data must be stored in a binary, not text, format. Protected personal information shall be stored in an encrypted format using at least a 128-bit key.

c. Release of Information

Explicit authority and permission from clients is required before basic identifiable client information can be released. Client information may also be released as permitted under Medicaid, state, and federal statutes. In addition, the clients have the right to have access to their own data.

- A Client Consent-Release of Information for Data Sharing form must be signed by a client upon intake (even to low-barrier shelters) before any information can be shared.
- All HMIS Participating Agencies will be required to follow all current data security practices detailed in the Policies and Procedures manual, and adhere to the ethical data use standards, regardless of the location where agency users connect to HMIS.
- The client will have access on demand to view, or keep a printed copy of, his or her own records contained in the HMIS.
- A privacy notice shall be prominently displayed in the program offices where intake occurs. The content of this privacy notice shall be in accordance with *HMIS Data and Technical Standards Notice* of July 30, 2004.
- An individual has the right to receive an accounting of disclosures of protected personal information made by a HMIS user or developer in the six years prior to the date in which the accounting is requested, except for disclosures for national security or intelligence purposes or to correctional institutions or law enforcement officials.
- Each Continuum of Care is required to have a written policy governing its use and disclosure of information collected by HMIS.

d. Client Consent to Share Data

Clients must be informed about the intended use of personal client information at the time the information is collected. Agencies are responsible for having the proper procedures in place to ensure the consent to use the information in the intended manner is understood by the client.

- A verbal explanation should include a description of NJ HMIS, how the information will be used, how it will be protected, and the advantages of providing accurate information.
- The consent procedure should document the information being shared and with whom it is being shared. After the consent procedure has been explained, the provider should request client to sign the Consent form.
- It is critical that every agency post at the intake area the NJ HMIS Collaborative's "Reason for collecting Protected Personal Information" Poster.
- The user is then responsible for checking the appropriate box on the intake form within the AWARDS system indicating which option of sharing the client has chosen.

e. HMIS Security

System Administrators and Site Administrators are responsible for validating, establishing, and granting security permissions and making sure security procedures are followed.

- Each agency is responsible for administering its own users (e.g., setting up user IDs, passwords, etc.).
- The System Administrator will provide a user ID and temporary password for each Site Administrator.
- The Site Administrators will provide a user ID and temporary password for each agency user.
- User names will be unique for each user.
- The System Administrator will have access to the complete list of users.
- The Site Administrator is responsible for terminating former employees.
- Any paper or other hard copy generated by or for HMIS that contains identifiable information must be under constant supervision by an HMIS user or developer when in a public area. When staff members are not present, the information shall be secured in areas that are not publicly accessible.
- Written information, specifically pertaining to user access (user name and password) shall not be stored or displayed in any publicly accessible location.

User IDs and Passwords

Password protection has been used for many years to control access to computer information. Your computer password is your personal key to a computer system. Passwords help to ensure that only authorized individuals access computer systems. Passwords also help to determine accountability for all transactions and other changes made to system resources, including data. If you share your password with a colleague or friend, you will be giving an unauthorized individual access to the system.

The relevant authorized user(s) will be held responsible if an unauthorized individual uses their access privileges to damage the information on the system or to make unauthorized changes to the data.

Simple rules for passwords

- Passwords should be kept confidential and should never be shared.
- Passwords should not be written down.
- Never use the same password twice. When you are selecting a new password, choose one that is quite different from your previous password.
- AWARDS passwords must be a minimum of eight characters.
- Passwords should not be trivial, predictable, or obvious.
- *Obvious* passwords include names of persons, pets, relatives, cities, streets, your user ID, your birth date, car license plate, and so on.
- *Predictable* passwords include days of the week, months, or a new password that has only one or two characters different from the previous one.
- *Trivial* passwords include common words like 'secret', 'password', 'computer', etc.
- Your password should not be the same as your user ID.

Rules for User IDs and Passwords

- DO NOT share your password with anyone else.
- DO NOT use someone else's ID or password. If you need more access than you presently have or if you are having problems with your access, contact your Site Administrator for help.
- DO NOT use obvious, trivial, or predictable passwords. Obvious, predictable and trivial passwords include: names of relatives or pets; street names; days and months; repetitive characters; dictionary words; and common words such as PASSWORD, SECURITY, SECRET, etc.
- BEWARE of "shoulder surfers". These are people who stand behind you and look over your shoulder while you are keying in your password or PIN, or while you are working with confidential information.
- DO NOT use your access level to enable other individuals to access information that they are not authorized to access, or to submit transactions that they are not authorized to submit.
- NEVER write down your passwords or post them on your terminal or other obvious places.
- ALWAYS change the initial password assigned to you by your administrator as soon as you receive it.
- LOG OFF when you are finished using your terminal or workstation, or if you are stepping away from your desk, even momentarily.
- If you are going to be away from the office for an extended period

- (e.g., maternity leave or vacation), ask your Site Administrator to get your ID temporarily suspended. Your ID will be reactivated when you return.

f. Data Access Location

Users should use precautions when accessing NJHMIS via the Web from public locations where the potential exists for viewing of client information by unauthorized persons.

g. Ethical Data Use

Every user bears primary responsibility for the material he or she chooses to access, store, print, send, display, or make available to others.

Appropriate use of the NJ HMIS modules includes, for example:

- Respect for the rights of others
- Respect for the property of others
- Consideration of other persons using shared systems
- Confidentiality in use of passwords and personal identification numbers
- A presumption of the right to privacy
- Use of tools for the purpose for which they are intended
- Adherence to the etiquette and culture as defined in systems that you use

Inappropriate use of the HMIS modules includes, for example:

- Unauthorized access, alteration, destruction, removal, and/or disclosure of data and/or information
- Disclosure of confidential passwords or personal identification numbers
- Malicious or unethical use, and use that violates federal laws

h. Security Audits

The NJHMIS Technical Assistants will perform regular security audits to ensure the security of HMIS data.

Access to HMIS

On your Web browser type:

https://njhmis.footholdtechnology.com

a. HMIS Customization

- Agencies may request more user licenses, custom reports, and interagency data integration products.
- Agencies will not be able to customize HMIS itself. However, agencies will be able to request additional reports, provide changes to the reports, and request software changes.
- If an agency chooses a system(s) other than the AWARDS system to collect HMIS data, that agency is responsible for customizing and maintaining that system(s).

b. Agency Participation Fee

- Each Participant will be charged an annual participation fee to be involved in the NJHMIS Collaborative. The annual fee will be invoiced and payable to the NJHMFA. The initial annual fee in the amount of five hundred ($500.00) dollars is due prior to the Participant's activation in the NJHMIS system. The annual fee is subject to change, and is the sole discretion of the NJHMFA.

c. User Activation

- Each user will be provided with a user ID and temporary password by the System Administrator or Site Administrator.
- The Site Administrator will take full responsibility for ensuring that their respective agency users are trained on the use of the HMIS modules, and that the user has knowledge of all HMIS policies and procedures.

d. Breach of System or Client Confidentiality Penalty

- Any Agency that is found to have had breaches of system security and/or client confidentiality shall enter a period of probation, during which time technical assistance shall be provided to help the Agency prevent further breaches.
- Probation shall remain in effect until the NJHMIS Project Manager has evaluated the Agency's security and confidentiality measures and found them compliant with the policies stated in this Agreement and the User Policy, Responsibility Statement, and Code of Ethics Agreement.
- Subsequent violations of system security will result in suspension from the system.

Hardware

NJ HMIS Collaborative Hardware Technical Specifications

The following information are for those agencies looking to purchase new hardware. These are not hardware requirements for using AWARDS. The AWARDS application is a web base system, which does not load any software onto your local machines. If your current system has Internet access you will be able to access AWARDS.

1. Minimum Recommendations for computer equipment/software.

PIII w/256k RAM

Microsoft Windows 98 or above with IE Browser

Communication

Ethernet RJ45 connection - Cable/DSL

Or

Phone Line - RJ11 connection

10 Gig Hard drive (not required for AWARDS, for agency use only)

CD-ROM Drive

2. Recommended software for your local desktop computers.
   This software is not required for AWARDS, but would help protect your local computers.
   Antivirus
   Spy ware or Spam Blocker

3. Recommended software for your local servers.
   This software is not required for AWARDS, but would help protect your servers.
   Antivirus
   Firewall
   Spy ware or Spam Blocker

(Look to Techsoup.com for non-profit costs on software.)

a. Participating Agency Hardware/Software Requirements

New Jersey's HMIS implementation will require agencies to have a minimum of one Personal Computer ("PC hardware") with Internet connectivity, preferably high-speed – cable, broadband, etc. ("communication hardware"); and one printer ("print hardware"). For the purposes of this document, "HMIS Hardware" refers to all of the above three categories of hardware.

b. Participating Agency Technical Support Requirements

Participating agencies are responsible for providing their own technical support for all hardware and software systems used to connect to HMIS.

- Ongoing maintenance and support of Personal Computer and Printer hardware will also be the responsibility of the agency.
- Personal Computer and Printer hardware support will be limited to product warranty directly from the manufacturer. Agencies agree to deal directly with manufacturer(s) during product warranty periods.
- New Jersey's HMIS Implementation is not responsible for any hardware or software upgrades, replacements, or warranty. Agencies will be required to ensure that the supplied hardware continue to meet the minimum standards prescribed by the HMIS application vendor.
- Communication and Internet connection difficulties will be managed between the agencies and the appropriate Internet Service Provider selected by that agency.
- The HMIS Help Desk will provide troubleshooting and problem analysis/triage related to HMIS application usage. If any difficulty is traced to agency hardware or agency Internet connection, the HMIS Help Desk will not be obligated to interface directly with any hardware manufacturer and/or ISP. The HMIS Help Desk will attempt to continue to support and assist the agencies until resolution of the issue/problem, but the primary responsible entity for resolving hardware and Internet communication problems will be the agency. The HMIS Help Desk will be the primary responsible entity for resolving application-specific HMIS problems.

New Jersey HMIS Required Data Elements

a. Required Data Collection

Each agency will be required to collect all data elements as listed below. An agency is responsible for what data they enter into HMIS beyond the HUD HMIS Required Data Elements.

UNIVERSAL DATA ELEMENTS

* Name
* Social Security number
* Date of birth
* Ethnicity and race
* Gender
* Veteran status
* Disabling condition
* Residence prior to program entry
* Zip code of last permanent address
* Program entry date
* Program exit date

Program-Specific Data Elements:

* Income and sources
* Non-cash benefits
* Physical disability
* Developmental disability
* HIV/AIDS
* Mental health
* Substance abuse
* Domestic violence
* Services received
* Destination
* Reasons for leaving
* Employment
* Education
* General health status
* Pregnancy status
* Veterans' information
* Children's education

Details about each of these categories may be read in HUD's Federal Register Final Notice FR 4848-N-02 dated July 30, 2004. The relevant pages are 45905-45927.

LISTING OF AWARDS INTAKE SCREEN ELEMENTS AND THEIR REQUIRED RESPONSES:

(All required elements have an Asterisk next to them)

Intake Date: (MM/DD/YY)
Shelter Bed:
Primary Worker
Referred by:
First Name*:
Middle Name:
Last Name*:
Suffix:
Alias:
Birth Date*: (MM/DD/YY)
Social Security #*: (999-99-9999 if unknown)
SSN Data Quality*:
1 = Full SSN reported.
2 = Partial SSN reported.
3 = Don't know or don't have SSN.
4 = Refused.
Gender*:
Male
Female
Trans-Male
Trans-Female
Ethnicity*:
0 = Non-Hispanic/Latino.
1 = Hispanic/Latino.
Race*: (multiple choices)
1 = American Indian or Alaska Native.
2 = Asian.
3 = Black or African-American.
4 = Native Hawaiian or Other Pacific Islander
5 = White
Chronically Homeless*:
Yes
No
Date Left Last Permanent Residence:
Zip Code of Last Permanent Address*:
Zip Code Data Quality*:
1 = Full Zip Code Recorded.
8 = Don't Know.
9 = Refused.
Residence Prior to Program Entry*:
1 = Emergency shelter (including a youth shelter, or hotel, motel, or campground paid for with emergency shelter voucher).
2 = Transitional housing for homeless persons (including homeless youth).
3 = Permanent housing for formerly homeless persons (such as SHP, S+C, or SRO Mod Rehab).
4 = Psychiatric hospital or other psychiatric facility.

5 = Substance abuse treatment facility or detox center.
6 = Hospital (non-psychiatric).
7 = Jail, prison or juvenile detention facility.
8 = Room, apartment, or house that you rent.
9 = Apartment or house that you own.
10 = Staying or living in a family member's room, apartment, or house.
11 = Staying or living in a friend's room, apartment, or house.
12 = Hotel or motel paid for without emergency shelter voucher.
13 = Foster care home or foster care group home.
14 = Place not meant for habitation (e.g., a vehicle, an abandoned building, bus/train/subway station/airport or anywhere outside).
15 = Other.
16 = Don't Know.
17 = Refused.

Length of Stay at Previous Residence*:

1 = One week or less.
2 = More than one week, but less than one month.
3 = One to three months.
4 = More than three months, but less than one year.
5 = One year or longer.

Marital Status*:

Single
Married
Common Law
Divorced
Separated
Remarried
Widow(er)

Individual/family Type*:

Individual Male
Individual Female
Individual Male Youth (< 18)
Individual Female Youth (< 18)
Single Parent Family - Male Head
Single Parent Family - Female Head
Single Parent Family - Youth Head
Two Parent Family - Adult
Two Parent Family - Youth
Adult Couple without Children

# of Children*: 0-9 (if greater than zero, age and gender for each child)

Income Sources*: (check all appropriate sources and enter dollar amount)

1 = Earned Income
2 = Unemployment Insurance
3 = Supplemental Security Income or SSI
4 = Social Security Disability Income (SSDI).
5 = A veteran's disability payment
6 = Private disability insurance
7 = Worker's compensation
8 = Temporary Assistance for Needy Families (TANF)
9 = General Assistance (GA) (or use local program name).
10 = Retirement income from Social Security
11 = Veteran's pension
12 = Pension from a former job
13 = Child support
14 = Alimony or other spousal support

15 = Other source
16 = No financial resources.

Non-Cash Benefits:

1 = Food stamps or money for food on a benefits card
2 = MEDICAID health insurance program (or use local name)
3 = MEDICARE health insurance program (or use local name)
4 = State Children's Health Insurance Program (or use local name)
5 = Special Supplemental Nutrition Program for Women, Infants, and Children (WIC)
6 = Veteran's Administration (VA) Medical Services
7 = TANF Child Care services (or use local name)
8 = TANF transportation services (or use local name)
9 = Other TANF-funded services (or use local name)
10 = Section 8, public housing, or other rental assistance
11 = Other source

Disabling Condition*:

Yes
No
Don't Know

General Health:

1 = Excellent
2 = Very good
3 = Good
4 = Fair
5 = Poor
8 = Don't Know

Currently Pregnant*:

Yes
No
(If Yes, Due date: MM/DD/YY)

Special Needs: (Check all that apply)

Mental Illness
Alcohol Abuse
Drug Abuse
HIV/AIDS
Mental Retardation/Development Disability
Domestic Violence
Other: (specify)

If Yes to Mental Illness:

Expected to be of long-continued and indefinite duration and substantially impairs ability to live independently:

Yes
No

If Yes to Drug/Alcohol Abuse:

Expected to be of long-continued and indefinite duration and substantially impairs ability to live independently:

Yes
No

If Yes to Domestic Violence, when did experience occur:

1 = Within the past three months
2 = Three to six months ago

3 = From six to twelve months ago
4 = More than a year ago
8 = Don't know
9 = Refused

Employment Status*:

Yes
No

# of Hours worked in the past week: (#)

Employment Tenure:

1 = Permanent
2 = Temporary
3 = Seasonal

Looking for Work (if not currently employed):

Yes
No

Highest Level of School Completed*:

0 = No schooling completed
1 = Nursery school to 4th grade

2 = 5th grade or 6th grade
3 = 7th grade or 8th grade
4 = 9th grade
5 = 10th grade
6 = 11th grade
7 = 12th grade, No diploma
8 = High school diploma
9 = GED
10 = Post-secondary school

Current Student*:

Yes
No

Post-Secondary Degree *:

None
Bachelors
Associates
Masters
Doctorate
Other graduate/professional degree

Received vocational training or apprenticeship certificate*:

Yes
No

Veteran's Status*:

Yes
No
Don't Know
Refused

Birth Place:

Citizen:

US Citizen

Registered Alien
Undocumented Alien

Alien Registration:

Homeless Cause

Homeless Duration:

Previous Living Situation*:

Rental Housing
Streets
Correctional
Psychiatric Facility
Emergency Shelter
Transitional Housing
With Family or Friends
Treatment Facility
Others
Own Home

Primary Language:

English
Spanish
French
Chinese
Arabic
Hebrew
Hindi
Russian
Sign Language
Other
Creole
Greek
Italian
Japanese
Vietnamese
Braille

Services Sought: (check all that apply)

Shelter/Housing

Drug Treatment

Mental Health Care

Medical Care

Legal Aid - CRJS/Civil

Legal Aid – immigration

Emergency Contact

Address

Relation:

Grandparent
Parent
Stepparent
Sibling
Guardian
Uncle
Aunt
Spouse

In-Law
Cousin
Friend
Provider

Phone:

LISTING OF AWARDS <u>DISCHARGE</u> SCREEN ELEMENTS AND THEIR REQUIRED RESPONSES:

(All required elements have an Asterisk next to them)

Resident: ***(displayed)***
Gender: ***(displayed)***
Birth Date: ***(displayed)***
Admission: ***(displayed)***
Address: ***(displayed)***
Referral Source: ***(displayed)***
Discharge Date*: (MM/DD/YY)
Reason for Discharge*:

Left for a housing opportunity before completing the program.
Completed program.
Non-payment of rent/occupancy charge
Non-compliance with project
Criminal activity / destruction of property / violence
Reach maximum time allowed in project
Needs could not be met by project
Disagreement with rules/persons
Death
Other
Unknown/disappeared

Monthly Income At Discharges: (Displayed from income choices below)
Income Sources*: (check all appropriate sources and enter dollar amount)

1 = Earned Income
2 = Unemployment Insurance
3 = Supplemental Security Income or SSI
4 = Social Security Disability Income (SSDI).
5 = A veteran's disability payment
6 = Private disability insurance
7 = Worker's compensation
8 = Temporary Assistance for Needy Families (TANF)
9 = General Assistance (GA) (or use local program name).
10 = Retirement income from Social Security
11 = Veteran's pension
12 = Pension from a former job
13 = Child support
14 = Alimony or other spousal support
15 = Other source
16 = None.

Non-Cash Benefits:

1 = Food stamps or money for food on a benefits card
2 = MEDICAID health insurance program (or use local name)
3 = MEDICARE health insurance program (or use local name)
4 = State Children's Health Insurance Program (or use local name)
5 = Special Supplemental Nutrition Program for Women, Infants, and Children (WIC)
6 = Veteran's Administration (VA) Medical Services
7 = TANF Child Care services (or use local name)
8 = TANF transportation services (or use local name)
9 = Other TANF-funded services (or use local name)
10 = Section 8, public housing, or other rental assistance

11 = Other source

New Residence Setting*:

1 = Emergency shelter (including a youth shelter, or hotel, motel, or campground paid for with emergency shelter voucher).
2 = Transitional housing for homeless persons (including homeless youth).
3 = Permanent housing for formerly homeless persons (such as SHP, S+C, or SRO Mod Rehab).
4 = Psychiatric hospital or other psychiatric facility.
5 = Substance abuse treatment facility or detox center.
6 = Hospital (non-psychiatric).
7 = Jail, prison or juvenile detention facility.
8 = Room, apartment, or house that you rent.
9 = Apartment or house that you own.
10 = Staying or living in a family member's room, apartment, or house.
11 = Staying or living in a friend's room, apartment, or house.
12 = Hotel or motel paid for without emergency shelter voucher.
13 = Foster care home or foster care group home.
14 = Place not meant for habitation (e.g., a vehicle, an abandoned building, bus/train/subway station/airport or anywhere outside).
15 = Other.
16 = Don't Know.
17 = Refused.

Destination Tenure*:

1 = Permanent
2 = Temporary
3 = Don't Know
4 = Refused.

Destination Subsidy Type*:

1 = None
2 = Public Housing
3 = Section 8
4 = S+C
5 = HOME Program
6 = HOPWA Program
7 = Other Housing Subsidy
8 = Don't Know
9 = Refused.

New Residence County*:

01 Atlantic
02 Bergen
03 Burlington
04 Camden
05 Cape May
06 Cumberland
07 Essex
08 Gloucester
09 Hudson
10 Hunterdon
11 Mercer
12 Middlesex
13 Monmouth
14 Morris
15 Ocean
16 Passaic
17 Salem
18 Somerset

19 Sussex
20 Union
21 Warren
70 NJ-Unknown
80 USA Not NJ
90 Non USA
99 Unkown

Discharge To:
Anonymous Summary:
Discharge Notes:
Service Charge:
Discharge Summary:
Alerts:
Known Medical Problems: (Displayed)
Counselor: (Displayed)
Supervisor: (Displayed)

b. Appropriate Data Collection

An agency is responsible for what data they enter into HMIS beyond the HUD HMIS Required Data Elements.

Quality Control

a. **Data Integrity**

HMIS users at the agencies are responsible for the accuracy, correctness, and timeliness of their data entry and are responsible for ensuring that the HUD HMIS Required Data Elements are being collected.

Site Administrators are responsible for monitoring the integrity of data being entered into the NJ HMIS system.

b. Data Integrity Expectations

Data entry into AWARDS must take place, at minimum, on a weekly basis.

- Data from across agencies will be synchronized on a weekly basis for reporting purposes.

Data Retrieval

a. Participating Agencies

- Interagency and inter-program data will be integrated under HMIS.
- While agencies are required to report a minimum data set on a regular basis, sharing of HMIS data among providers within the CoC is encouraged, but not required and is at the discretion of each client.
- Access to interagency identifiable information will only occur as authorized under state and/or federal statutes or via a Release of Information form signed by the client. Sharing data to determine service needs would therefore be facilitated.

b. HMIS Software Provider

The HMIS Software Provider does have access to individual and aggregate data contained within the HMIS. They will be responsible for addressing and resolving all issues that cannot be resolved at the local level.

c. General Public

The general public has a right to request non-identifiable aggregate data related to homelessness.

User Licenses

a. Software Licenses

- Each agency will receive one user license per user for users to access the NJ HMIS system via the Internet.
- The Site Administrator will be responsible for tracking and reporting on utilization of user licenses. Unused licenses must be reported to the System Administrator.

.

Data Loading

a. Client Data

- NJHMIS provides for the loading and sharing of client information.
- Historical client information, if possible and existing on a legacy MIS system, will initially be migrated to NJHMIS on a one time basis.
- Client data in Foothold Technology AWARDS will be available real-time, assuming that agency data is entered real-time.
- NJHMIS will provide a mechanism to load client data from existing agency MIS systems (i.e., any large scale third or fourth generation database systems) into the NJHMIS system.

b. <u>Schedule of Data Loads</u>

- NJHMIS data loads will take place weekly.
- NJHMIS users with data sources other than Foothold Technology AWARDS are encouraged to upload data weekly. However, every agency must upload their data by final business day of each month.
- Although data loads take place weekly, agencies can enter data into NJHMIS in real-time.

Training

a. HMIS Train-the-Trainer

- Train-the-Trainer is a concept whereby someone is trained on how to teach others to complete a certain task.
- The person charged with this responsibility of train the trainer for your facility will be given the security level of "HMIS Site Administrator".
- The HMIS Train-the-Trainer will be responsible for training all End Users for his/her respective agency.

b. Ongoing HMIS Training

- The HMIS Site Administrator will be provided with necessary training, a written course outline, and available training materials. NJ HMIS Collaborative will provide periodic refresher courses for Site Administrators.
- If an end user leaves an agency, the HMIS Site Administrator is responsible for ensuring that the new person will be trained.

c. Training Materials for Future Releases

The HMIS Site Administrator will be provided with necessary training, a written course outline and available training materials.

APPENDIX:
Roles and Responsibilities

a. System Administrator

- As the lead agency, the New Jersey Housing Mortgage Finance Agency (NJ HMFA) will employ the System Administrator for the purpose of coordinating access control requirements for all AWARDS users. The System Administrator will be a member of the Advisory Council, Steering Committee, and any subcommittees.
- NJ HMFA will ensure that a backup to the System Administrator is in place, in order to ensure that there is no interruption of service when the primary representative is away or unavailable to assist users.

Responsibilities

- Ensure that the Site Administrator has proper access level to the system.
- Chair the Advisory Council and reporting relevant issues to the Steering Committee.
- Implement decisions made by the Steering Committee.
- Assist Site Administrators with access problems, including:
    - Reissue passwords when the Site Administrator or user forgets their password.
    - Assist Site Administrators with questions and/or problems with the system.
- Delete access when Site Administrators are terminated or when they leave an agency.
- Ensure that users are aware of security requirements and policies and procedures.
- Inform Site Administrators when either the AWARDS data entry portal or the reporting portal is out of service.

b. HMIS Technical Assistant

- The lead agency (NJ HMFA) will employ the Technical Assistant.
- This person will report to the System Administrator / HMIS Project Manager.
- The Technical Assistant will be a member of the Advisory Council and will serve, as backup to the System Administrator to ensure that there is no interruption of service when the primary representative is away or unavailable to assist users.
- Will act as a liaison between NJ HMFA and the CoC HMIS subcommittees.

Responsibilities

- Ensure that the Site Administrator has proper access level to the system.
- Chair the Advisory Council and reporting relevant issues to the Steering Committee.
- Assist Site Administrators with access problems, including:
    - Reissue passwords when the Site Administrator or user forgets their password.
    - Assist Site Administrators with questions and/or problems with the system.
- Delete access when Site Administrators are terminated or when they leave an agency.
- Ensure that users are aware of security requirements and policies and procedures.
- Inform Site Administrators when either the AWARDS data entry portal or the reporting portal is out of service.
- Responsible for providing HMIS training to Site Administrators and end users.
- Provide second-level help desk support. If required, communicate issues to the AWARDS technical staff for resolution.

c. System Administrative Assistant

The lead agency (NJ HMFA) will employ the Program Administrative Assistant with the purpose of coordinating and disseminating information to all AWARDS users. This person will report to the System Administrator / HMIS Project Manager.

Responsibilities

- Take minutes at all NJ HMIS meetings and distributing the minutes to the appropriate people.
- First-level help desk support. This includes:
  - Answering the help desk 800 number
  - Documenting and distributing help desk related issues
  - Escalating help desk issues if unresolved
- Disseminate any NJ HMIS-related documents or information.
- Coordinate and scheduling meetings and trainings.
- Perform other duties as required.

d. Site Administrator

- A Site Administrator will be designated by each provider for the purpose of coordinating access control requirements for users within their agency only.
- It is recommended that a backup to the Site Administrator be designated in order to ensure that there is no interruption of service when the primary representative is away or unavailable to assist users.

Responsibilities

- Coordinate access control requirements for users within their agency.
- Assist users with access problems, including:
    - Contacting the System Administrator on behalf of users who forget their password
    - Helping new users with logon procedures
- Inform the System Administrator when any of their users leave the agency.
- Assign the user access level.
- Delete access when users are terminated or when they leave the agency.
- Train all users within their agency to use the A.W.A.R.D.S system. The training should include any manuals, guidelines and other documents provided to them at their Train-the-Trainer sessions.
- Ensure that users are aware of security requirements, policies, and procedures.
- Periodically run and review audit reports to ensure appropriate privacy and data access policies are being followed by staff. Site Administrators can produce audit reports that report AWARDS user activity by user ID, time, date, and what client records were added, changed, or deleted.

e. Participating Agencies

Participating Agencies agree to use the NJHMIS for the purpose of homeless client intake and agree to collect the HUD-mandated minimum data set and enter this information into the NJHMIS system. The NJHMIS system may also be used for case management.

Responsibilities

- All participating agencies agree to abide by all policies and procedures outlined in this manual.
- All participating agencies agree to keep abreast of all AWARDS updates and all policy changes.
- Each agency will be responsible for identifying and approving their respective agency users.
- Each participating agency will be responsible for entering client data, following up on referrals, and running reports.
- All participating agencies are responsible for payment of their annual user fee to NJ HMFA.

f. NJ HMIS Steering Committee

- The NJ HMIS Steering Committee is responsible for HMIS-related policies and procedures, and for reviewing recommendations for approval from the NJ HMIS Advisory Council.

g. NJ HMIS Advisory Council

The NJHMIS Advisory Council will meet quarterly to discuss recommendations for system-wide changes in HMIS functionality and system-flow. The NJHMIS Project Manager will chair the Advisory Council.

The Advisory Council includes the following standing committees:

- Support Fund
- Training
- Policies and Procedures
- Data, Quality Assurance, and Outcome Measures
- Technology

Support Fund Committee-
Chair-
Purpose:

To develop criteria for the request of technology support funds by service providers participating in the Collaborative.

This criteria, would include specifics pertaining to, for example but not limited to, organization size and budget, technical capacity, funding limits, type of technology eligible for funding, frequency of which funds can be requested, obligation to collaborative for assistance. In addition, this committee will be charged with researching and providing information on funding/charitable resources interested in building the technological capacity of non-profit organization, making this information accessible to ALL provider agencies within the Collaborative.

Training Committee-
Chair-
Purpose:

Develop and provide a training strategy using Beta implementation as a baseline, providing recommendations for amendments and improvements for the remaining phases of implementation**.**

To maintain a pulse on the training needs of end users at the local level. This committee could develop a mechanism by which to regularly assess end users and executive agency staff's satisfaction with training provisions and make recommendations based on findings. Should work in concert with TA staff.

Policy and Procedures Committee
Chair-
Purpose:

Assess policy and procedures applied during the Beta phase, provide qualitative feedback on issues raised by the community users, what worked, what didn't, recommendations for changes.

This committee's charge is to make sure the policies and procedures of the HMIS Collaborative are not in direct conflict with local service provider agency's protocols, policies, and/or practices and that the same holds true with those of participating agencies in respect to HMIS and the HMIS Collaborative. This committee shall identify such conflicts and bring them forward for review and recommend resolution. This committee may find a need to develop a mechanism to identify areas of possible conflict and how to monitor for those as time moves forward. Will work with HMIS staff in policy changes made at the federal level (HUD) on HMIS, specifically when the changes will impact the providers at the local level.

Data, Quality Assurance, and Outcome Measures
Chair-
Purpose:

To gather feedback from end users during pilot phase to establish a consensus for needed and/or desired customizations.

To keep abreast of data standards and changes required by HUD in regard to HMIS. To assess issues at the local level that impact data collection and quality. Make recommendations based on assessments. To review outcome measures being used by other HMIS communities to date, determine what outcomes the NJ State HMIS Collaborative would usefully measure.

Technology
Chair-
Purpose:

To develop technical specification criteria to be used in conjunction with the criteria for need (established by the Support Committee), to determine technical purchases by local agencies with funds granted by the Collaborative Support Fund.

Develop an assessment tool for the evaluation of HMIS technical infrastructure. Evaluate issues regarding the importation and exportation of data.

h. HMIS User

NJ HMIS users are those individuals who work in Participating Agencies.

Responsibilities

- Each user will be responsible for complying with all the policies and procedures outlined in this manual.
- Each user will be responsible for using the NJ HMIS in an appropriate and ethical manner.

i. HMIS User Access Levels

Determination of HMIS user access levels will be based on each user's job function as it is related to AWARDS's data entry and retrieval schema. The following access levels are available in AWARDS. All levels are not required. Levels should be used based on each agencies organization structure.

Access Level	Description
HMIS Project Manager (CoC Executive Officer)	Access is generally limited to the de-identified database. This role allows the user to search the de-identified database of area agencies and programs to view or produce reports of the aggregated data. Sometimes the HMIS Project Manager may have to access the identifiable database for support purpose.
Technical Assistant/Trainer (CoC Executive Officer)	The same access rights as HMIS Project Manager, however, this person is considered a system-wide Support person and will have access to client level data to facilitate supporting agency problems.
Volunteer (Direct Care Staff)	Access is limited to service records within an agency. A volunteer can view or edit basic demographic information about clients (the profile screen), but is restricted from viewing detailed assessments. A volunteer can enter new client records; make referrals, or check-in/out a client from a shelter. Normally, this access level allows a volunteer to complete the intake and then refer the client to agency staff or a case manager.
Agency Clerical Staff (Direct Care Staff)	Agency staff has full access to service records and access to most functions in AWARDS. However, Agency Staff can only access basic demographic data on clients (profile screen). All other screens are restricted, including assessments and case plan records.
Case Manager (Direct Care Staff)	Case Managers have access to all features, excluding administrative functions. They have access to all screens within AWARDS, including assessments and service records. There is full reporting access.

Site Administrator (Agency Executive)	Site Administrators have access to all features, including agency level administrative functions. This level can add/remove user for his/her agency and edit their agency and program data. They have full reporting access.
Executive Director (Agency Executive)	Same access rights as Site Administrator, but ranked above Site Administrator.

Access Level	Description
Regional or CoC Administrator (Agency Executive)	Regional or CoC Administrator will help to maintain the AWARDS system, but does not have access to client or service records, add/remove users, reset passwords, and access to other system-level options for agencies within their jurisdiction. They can search the de-identified database and produce reports of the aggregated data. They will not have access to client level data.

h. <u>Communication with Participating Agencies</u>

- Operational procedures will need to be enforced.
- Each agency is responsible for making sure that all necessary NJ HMIS-related communication occurs.

i. System Availability

- The AWARDS data entry portal will be available 24 hours a day, 7 days a week.
- Agency and System Administrators will be informed of any operational downtime.

j. <u>Client Grievance</u>

- NJ HMIS itself does not intend to create or establish any unique grievance management processes.
- All agencies are responsible for setting up an internal grievance process to handle client complaints related to HMIS, including grievances related to consent and release of information.