

NEW JERSEY HOMELESS MANAGEMENT INFORMATION SYSTEM
Policies & Procedures Manual

Introduction

New Jersey's HMIS is a collaborative effort between the New Jersey Housing Mortgage Finance Agency (HMFA), the dedicated lead agency, and 19 counties that make up New Jersey's (15) Continuum of Care (CoC). The Continuum of Care, individually or as a group, has 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 Continuum of Care retains the right to withhold support for HMIS.

New Jersey's HMIS project is governed by an HMIS Advisory Council, which will include representatives from NJ HMFA and representatives from each CoC.

Atlantic County CoC
Bergen County CoC
Burlington County CoC
Camden/Gloucester/Cape May/Cumberland Counties CoC
Newark/Essex County CoC
Jersey City, Bayonne/Hudson County CoC
New Brunswick/Middlesex County CoC
Monmouth County CoC
Morris County CoC
Lakewood Township/Ocean County CoC
Paterson/Passaic County CoC
Salem County CoC
Trenton/Mercer County CoC
Elizabeth/Union County CoC
Warren, Sussex, Hunterdon Counties CoC

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.

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

For more information regarding NJHMIS Policies and Procedures, please contact Catherine Brewster, New Jersey Housing Mortgage Finance Agency, at 609-278-7567 or cbrewster@njhmfa.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 Health Insurance Portability and Accountability Act (HIPAA) standards
- Baseline standards required by any organization that records, uses, or processes Personal Identifying Information (PII) on homeless clients for a HMIS. Additional protocols or policies to enhance further privacy & security for individual agencies, as deemed 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 the nature of homeless population

Section 4.1.1 Definition of Terms

Housing and Urban Development (HUD) is a federal government agency that supports affordable housing and community development by administering programs that provide housing assistance and promote fair housing

Homeless Management Information System (HMIS) is an electronic data collection system that stores project-level and client-level information about homeless persons who access a community's homeless service system.

Continuum of Care (CoC) is a regional planning body comprised of various organizations that collaborate to plan and coordinate services for people experiencing homelessness, aiming to end homelessness by providing a strategic system of housing and services

Personal Identifying Information (PII) – 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 PII on homeless clients for a HMIS

Processing operation or set of operations performed on PII for collection, maintenance, use, disclosure, transmission & destruction of information

HMIS Uses and Disclosures – uses and disclosures allowed by these standards.
Public Key Infrastructure (PKI) is a framework of hardware, software, policies, and procedures that enables trusted digital communications by managing public keys and digital certificates

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

Section 4.1.3 Allowable HMIS uses & disclosures of PII

- Allowable uses: 1) provide or coordinate services; 2) services related to payment or reimbursement; 3) carry out administrative functions; 4) create de-identified PII.
- 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 is limited to the requirements of law
    - If the client agrees to disclosure
    - Authorized by statute or regulation; necessary to prevent serious harm or if the individual is incapacitated and not intended to be used against the individual
    - Must inform the individual that a report has been made;
- Uses and disclosures for academic research; must be a formal relationship. Disclosures for law enforcement purposes: court order, warrant, subpoena, or summons.

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 PII; responsibility for privacy & security by both organizations; must comply with HMIS standards and allow for un-duplication of homeless clients at the CoC level

Section 4.2.1 Collection Limitation

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

Section 4.2.2 Data Quality

- PII 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 the purposes for collecting PII 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 the request of the individual
    - Limiting uses/disclosures as stated in the privacy notice
    - No disclosure of PII unless required by statute
    - Maintain audit trail containing date, purpose & recipient
    - Make audit trails available to homeless individuals
    - Limit disclosure of PII to the minimum necessary for the 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 the 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 the data collection process.
- Provide required information in languages other than English, common to the community
- Additional Privacy Protections-**See section for further discussion**

Section 4.2.5 Access and Correction

- Must allow the client to inspect and obtain a copy of any PII about the client
- Must explain any questions
- Must consider any request by the client for correction of inaccurate or incomplete PII pertaining to the client
- A CHO is not required to remove PII information, may mark information as inaccurate or incomplete, and may make additions
- Privacy Notice may reserve the right to deny the client the right to inspect and obtain a copy
    - Litigation or comparable proceedings
    - Information about another individual
    - Promise of confidentiality, if disclosure would reveal the source of information
    - Information that would endanger the life or physical safety of an individual
- Upon denial to inspect or obtain a copy, CHO must explain the reason for the denial, including the request documentation as part of PII
- 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 a specific basis for denial
    - Allow the client to add disagreement to the PII and allow them to share disputed information with another person
    - Provide a written explanation of the 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 the privacy notice and pledging to comply with the privacy notice
- Additional Privacy Protections- 1) may request staff to undergo formal training in privacy requirements; 2) Establish a method for regularly reviewing compliance with privacy notice; 3) Establish an 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 PII 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. The password must contain:

  1) 12-64 characters
  2) Contains letters and numbers
  3) Contains special characters
  4) Contains upper- and lower-case letters

  - Do not use your username, the NJHMIS name, or the HMIS vendor's 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 a public access area
  - Individual users must not have access to more than one workstation or log on to the network at more than one location at a time

- 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 the software vendor
- May commit to automatically scanning all files for viruses when the system is turned on, shut down, or not actively being used
- Must have a secure firewall between the workstation and any systems
- Modem access must have its own firewall

- Central server access, server must have a firewall
- Older operating systems may need to be equipped with secure firewalls
- Additional security protections-Apply a 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. 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 the workstation is temporarily not in use; the time for password protection can be regulated by CHO
- Staff should log off and shut down the data entry system when gone for an extended period
- All HMIS data must be copied to another medium regularly and stored in a secure off-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 the storage medium when deleting all HMIS data; reformat the storage medium more than once before reusing or disposing of 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
- All HMIS data must be stored in a binary, not text, format
- All paper or other hard copies containing PII for HMIS must be secured
    - Reports
    - Data entry forms
    - Signed consent forms
- All paper or other hard copies containing PII must be supervised at all times when in a public area

a. Personal Identifying 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 than a state, including street address, city, county, precinct, zip code, and their equivalent geo codes.
- 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 is 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 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. Personal Identifying Information shall be stored in an encrypted format using at least a 128-bit key.

c. <u>Release of Information</u>

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 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.
- If a client receives financial assistance, that information will become visible to all of the partner agencies, except public (county, state, or federal) agencies that make cash disbursements on behalf of clients.
- 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 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 the *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 before the date on 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. <u>Client Consent to Share Data</u>

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

- 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 the 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. <u>HMIS Security</u>

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 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 about 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.

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 the 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 the 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

In 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. A breakdown of the participation fee can be found in the APA. The annual fee is subject to change and is at 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 Director 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 is for those agencies looking to purchase new hardware. These are not hardware requirements for using AWARDS. The AWARDS application is a web-based 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 10 with Chrome or Firefox
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 the 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 continues 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 per the latest HUD HMIS Required Data Elements.

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.

b. Appropriate Data Collection

An agency is responsible for what data it enters 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

At a minimum on a weekly basis, but should aim towards HUD's standards of 3 business days. 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 terminated immediately.

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 in real-time, assuming that agency data is entered in 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.

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 training the trainer for your facility will be given the user group 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. Training information can be found on the following platforms.

YouTube: https://www.youtube.com/channel/UCaZRchtdY7H4CmY7sn1kdKA

AWARDS home screen: https://njhmis.footholdtechnology.com

Talent LMS: https://njhmis.talentlms.com

APPENDIX:
Roles and Responsibilities

a

i. <u>HMIS User Access Levels</u>

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 agency's organization structure.

Access Level	Description
HMIS Team Members (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 (Local CoC Admin)	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. <u>System Availability</u>

- 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.