NYC Coalition on the Continuum of Care

HMIS Policies and Procedures

Version 5

Effective: April 1, 2018

Table of Contents

Version and Review History

Version	Description	Data Management Committee Approved	Steering Committee Approved	Effective Date
1.0	Original Version	12/12/12	12/21/12	1/1/13
2.0	Updated to conform with DHS OIT standards	5/8/13	5/17/13	5/17/13
2.1	Updated (clerical corrections)	8/14/13	n/a	5/17/13
3.0	2014 Annual Update/ 2014 Data Standards compliance	8/8/14	9/19/14	10/1/14
4.0	2016 Annual Update/ 2016 Data Standards compliance	1/29/16	2/5/16	2/5/16
4.1	2017 Annual Update/ 2017 Data Standards compliance	N/A	N/A	7/1/17
5.0	2018 Annual Update/ 2017 Data Standards compliance	2/2/18	2/16/18	4/1/18

1. HMIS Overview

1.1. HMIS Governing Principles

In FY2001, Congress directed the U.S. Department of Housing and Urban Development (HUD) to ensure that homeless programs using federal funds utilize and participate in local homeless management information systems (HMIS) to track the use of services and housing within a continuum of care (CoC).[1]

The funded programs include:

- Emergency Solutions Grants (ESG) Program (formerly Emergency Shelter Grants Program)
- Continuum of Care (CoC) Program (formerly SHP and S+C)
- Housing Opportunities for People with AIDS (HOPWA) Program
- Veterans affairs Supportive Housing (VASH)

In addition, other federal entities have required HMIS participation for their homeless-related programs and grants. These include:

- Veterans Administration Grant Per Diem (GPD) Program
- Veterans Administration Community Contract Emergency Housing (CCEH)
- Veterans Administration Supportive Services for Veteran Families (SSVF) Program
- HHS - Substance Abuse and Mental Health Administration (SAMHSA) Projects for Assistance in Transition from Homelessness (PATH) Program
- HHS- Runaway and Homeless Youth Programs (RHY)

HUD requires all projects receiving funding through these programs to participate in HMIS. Projects that receive other sources of funding are not required to participate in HMIS, but both HUD and the New York City Coalition on the Continuum of Care (CCoC) strongly encourage them to do so to contribute to a better understanding of homelessness in our community by improving the HMIS participation rate. Any project that participates in the HMIS is subject to the data collection and management requirements outlined in these policies and procedures.

HMIS is essential to efforts to coordinate client services and inform community planning and public policy. Through HMIS, homeless individuals benefit from improved coordination within and among agencies, informed advocacy efforts, and policies that result in targeted services. Analysis of information gathered through HMIS is critical to the preparation of a periodic accounting of homelessness in New York City (NYC), including required HUD reporting. The Contributing HMIS Organizations (CHOs) recognize that thorough and accurate capture and analysis of data about homeless services and individuals is necessary to service and systems planning, effective resource allocation, and advocacy; therefore, they share a mutual interest in successfully implementing and operating HMIS in NYC.

1.2. HMIS Project Structure

The NYC CoC – as represented by the NYC CCoC –has designated the NYC Department of Social Services (DSS) acting on behalf of the NYC Department of Homeless Services (DHS) as the HMIS Lead Agency via a Memorandum of Understanding (MOU) to manage HMIS operations on its behalf and to provide HMIS Project administrative functions at the direction of the CCoC, through its Steering Committee.

The CCoC has selected a single product—Foothold Technology Service (FTS) AWARDS—to serve as the sole HMIS for the CoC. The HMIS Lead has established the NYC CCoC's HMIS as a Data Warehouse, meaning that participating agencies may upload data to the Data Warehouse from their project-level client management systems, so long as

[1] See HUD Strategy for Homeless Data Collection Conference Report (H.R. Report 106-988), which indicated that "local jurisdictions should be collecting an array of data on homelessness in order to prevent duplicate counting of homeless persons and to analyze their patterns of use of assistance, including how they enter and exit the homeless assistance system and the effectiveness of the systems. HUD is directed to take the lead in working with communities toward this end and to analyze jurisdictional data within three years."

those systems meet all applicable HUD and CCoC HMIS requirements as outlined in these policies and procedures, including the ability to export CSV files in the latest HMIS CSV standard format. That is to say, Agencies which use AWARDS as their client management system shall upload data using the AWARDS One-Button Upload feature. Agencies that use other HMIS-comparable client management systems must import data manually using the HMIS CSV file standards. Agencies that upload data to the Data Warehouse are considered CHOs. Agencies that are required to participate in HMIS by HUD or other federal entities will be considered to be meeting their participation requirements so long as they meet the standards outlined in **Section 3. CHO HMIS Participation Policies** of these policies and procedures. NYC DSS is responsible for ensuring the NYC-CARES system and users meet these standards.

1.3. HMIS Policies and Procedures Structure

These policies and procedures are structured in seven subsections:

- **Section 1. HMIS Overview:** provides an overview of the HMIS Project structure, key terms for the policies and procedures, and the HMIS project policy on data ownership.
- **Section 2. HMIS Project Administration and Management:** outlines the HMIS Project Administration, including the roles and responsibilities of the CCoC and its governance committees, and the HMIS Lead in managing the HMIS Project and the Data Warehouse. Detailed policies regarding the use of the Data Warehouse and grievances against the HMIS Lead are also provided in this section.
- **Section 3. CHO HMIS Participation Policies:** explains how an organization becomes a CHO, including describing the procedures for entering into **Appendix C. Organization HMIS Participation Agreement**, the roles and responsibilities associated with administering a CHO, and the technical and training requirements the CHO is required to demonstrate.
- **Section 4. HMIS Security Plan:** outlines the HMIS Lead Security Plan and details the minimum standards to which each CHO must adhere in order to maintain protected personal information securely.
- **Section 5. Disaster Recovery:** outlines the HMIS Lead Disaster Recovery Plan.
- **Section 6. Privacy Policy:** outlines the HMIS Lead Privacy Policy and details the minimum standards to which each CHO must adhere in using and disclosing client data.
- **Section 7. Data Quality:** outlines the HMIS Lead Data Quality Plan and details the minimum data collection and quality standards to which each CHO must adhere in their efforts to maintain accurate, complete, and timely data.
- Forms and documentation are provided in the appendices.

1.4. Key Terms

Annual Assessment	Data Collection Point that that is to be recorded no more than 30 days before or after the anniversary of the client's Project Entry Date, regardless of the date of the most recent update. Information must be accurate as of the Information Date.
Annual Performance Report (APR)	HUD project-level report that uses data about clients served and project performance.
AWARDS	A project-level HMIS-compliant system from which data can be uploaded directly to the Data Warehouse, AWARDS is a direct data entry software product owned by FTS. The NYC HMIS Data Warehouse uses AWARDS software.
Client	For the purposes of this policy, "client" refers to an individual or family residing in a shelter or housing project and/or recipients of services delivered by projects administered by a CHO.
Coalition on the Continuum of Care (CCoC)	The NYC group of representatives organized to carry out the responsibilities of a Continuum of Care as defined by HUD.
CCoC Data Management Committee	A committee of the NYC CCoC, the purpose of which is to provide support and recommendations to the NYC CCoC Steering Committee related to the HMIS regulations and standards as set forth by HUD.
CCoC Steering Committee	A committee of the CCoC charged with carrying out its oversight and governance responsibilities.

Continuum of Care	The group organized to carry out the responsibilities required under 24 CFR part 578 and that is composed of representatives of organizations, including nonprofit homeless providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve homeless and formerly homeless veterans, and homeless and formerly homeless persons to the extent these groups are represented within the geographic area and are available to participate.
Comma Separated Value (CSV)	Shorthand, used throughout this document, to refer to a HUD-approved data exchange standard, when performed consistent with current HUD HMIS CSV Format Documentation.
Contributing HMIS Organization (CHO)	An organization that operates a project that contributes data to the Data Warehouse consistent with all applicable HUD and local standards outlined in the NYC HMIS Policies and Procedures and **Appendix C. Organization HMIS Participation Agreement.**
CHO HMIS Administrator	A single point-of-contact established by each CHO who is responsible for day-to-day operation of the CHO data collection system, ensuring project-level data quality according to the terms of the **Appendix C. Organization HMIS Participation Agreement** and associated data quality plan, and managing the upload process from the CHO project-level HMIS-compliant system to the HMIS Data Warehouse.
CHO HMIS Security Contact	A single point-of-contact established by each CHO who is responsible for annually certifying that the CHO adheres to the Security Plan; testing the CHO security practices for compliance; communicating any security questions, requests, or security breaches to the DSS HMIS Director and Security Officer, and security-related HMIS information relayed from DSS to the CHO's End Users.
Contributing Data Warehouse User	CHOs enter data in to AWARDS or their own HMIS systems but do not actually touch the Data Warehouse. Rather, they "contribute" information to the Data Warehouse. Only the NYC DSS HMIS Team's version of AWARDS constitutes the actual Data Warehouse.
Data Warehouse	The NYC CCoC HMIS was established as a data warehouse, rather than as a direct data entry system. Thus, all CHOs are expected to regularly upload data, at intervals and through mechanisms specified in **Appendix C. Organization HMIS Participation Agreements**, to the Data Warehouse. The CCoC has selected a single product – Foothold Technology Services (FTS) – to serve as the Data Warehouse for the CCoC. The authority to enter into contracts with FTS for the purposes of operating and overseeing the HMIS Data Warehouse is the responsibility of the HMIS Lead Agency.
DHS	Working with multiple partners, the New York City Department of Homeless Services (DHS)' mission is to prevent homelessness when possible, to provide temporary shelter when needed, and to help individuals and families transition rapidly into permanent housing. As a result of the integration of some departments between DHS and HRA, including the CoC Unit, the CoC Unit now sits in DSS, and so DSS acts on behalf of DHS as the HMIS Lead and as a representative on the NYC CCoC.
DHS-CARES	A project-level HMIS-compliant system managed by DHS from which data is uploaded regularly to the Data Warehouse. DHS' Client Assistance and Re-Housing Enterprise System is an integrated case management system that gives DHS and provider staff the ability to serve and track clients from intake, to shelter placement and through their return to the community.

CHO End User	An employee, volunteer, affiliate, associate, or any other individual acting on behalf of a CHO or an HMIS Lead Agency who uses or uploads data in project-level HMIS-compliant system from which data are periodically uploaded to the HMIS Data Warehouse. Throughout this document, users will be specified as Data Warehouse End Users or CHO End Users.
Encryption	Encryption refers to the process of transforming information in order to make such information unreadable to anyone except those possessing special knowledge or a key.
FTS	Foothold Technology Service (FTS) is the vendor that operates NYC's HMIS system, AWARDS.
HMIS Data Dictionary	The HMIS Data Dictionary is designed for HMIS vendors and HMIS Lead Agency system administrators to understand all of the data elements required in an HMIS, data collection and function of each required element and the specific use of each element by the appropriate federal partner. The HMIS Data Dictionary should be the source for HMIS software programming.
HMIS Data Standards Manual	Published by HUD, the Data Standards Manual establish uniform definitions for the types of information to be collected and protocols for when data are collected and from whom. CHOs may have additional data collection requirements based on other funding sources, the client population served, and the types of data necessary to effectively monitor programs.
HMIS Lead Agency (HMIS Lead)	The entity – NYC DSS – designated by the CCoC to operate the HMIS Project in accordance with HUD standards.
HMIS Project	The system comprising the Data Warehouse, CHOs, project-level HMIS-compliant systems, and the policies and procedures that govern the relationship between these entities. The HMIS Project is managed by the HMIS Lead.
HMIS Director	The person responsible for administration of the HMIS Project and the Data Warehouse for the HMIS Lead; this user has full access to all user and administrative functions of the Data Warehouse and is responsible for organizational contact with the CHOs on matters related to the HMIS Project.
HMIS Team	Staff working in the NYC DSS CoC Unit under the direction of the HMIS Director
Housing for People with AIDS (HOPWA)	The Housing Opportunities Program (HOPWA) provides housing assistance and supportive services for low-income persons with HIV/AIDS and their families. Administered by the Department of Community Affairs, HOPWA enables eligible persons with HIV/AIDS and their families to secure decent safe and sanitary housing in the private rental market by subsidizing a portion of the household's monthly rent.
Housing Preservation and Development (HPD)	NYC Agency that protects the existing housing stock and expands housing options for New Yorkers as it strives to improve the availability, affordability, and quality of housing in NYC.
Information Technology	Means any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
Metadata Elements	Data about data elements documenting required metadata collection.
Office and Technology Resources	Includes but is not limited to: information technology, personal computers and related peripheral equipment, software, library resources, telephones, mobile telephones, pagers and other wireless communications devices, facsimile machines, photocopiers, Internet connectivity and access to Internet services, and email.

Office of Alcoholism and Substance Abuse Services (OASAS)	New York State Agency that plans, develops and regulates the state's system of chemical dependence and gambling treatment agencies. In addition, the Office licenses, funds, and supervises community-based programs, chemical dependence treatment programs. The agency inspects and monitors these programs to guarantee quality of care and to ensure compliance with state and national standards.
Office of Mental Health (OMH)	New York State Agency that operates psychiatric centers across the State, and also regulates, certifies and oversees programs, which are operated by local governments and nonprofit agencies. These programs include various inpatient and outpatient programs, emergency, community support, residential and family care programs.
Office of Temporary Disability Assistance (OTDA)	New York State Agency that provides temporary cash assistance; assistance in paying for food; heating assistance; oversees New York State's child support enforcement program; determines certain aspects of eligibility for Social Security Disability benefits; supervises homeless housing and services programs; and provides assistance to certain immigrant populations.
Personally Identifiable Information/ Protected Identifying Information (PII)	Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. Encompasses DHS Office of Information Technology (OIT) definition of "confidential information".
Personal Use	Means activity that is conducted for purposes other than accomplishing official work related activity.
Project Descriptor Data Elements	Required project level elements initially entered at the set-up stage of the project within an HMIS that specifically identify the organization, project name, continuum in which the project operated, type of project, bed and unit inventory for residential projects, and funding source.
Program -Specific Data Elements	Client level elements required by a specific federal program or program component. (**Section 7. Data Quality Plan** of these policies and procedures).
Project	A distinct unit of an organization, which may or may not be federally funded by HUD or the federal partners, that provides services and/or lodging and is identified by the CoC as part of its service system . Projects can be classified as providing lodging or services. Encompasses the DHS OIT term "provider," which refers to an agent who administers a program or delivers client services.
Project Entry	Data collection point indicating the element is required to be collected at every project entry. Elements collected at project entry must have an information date that matches the client's project entry date.
Project-level HMIS-Compliant System	A client management information system operated by a CHO that allows the CHO to collect the minimum required data elements and to meet other established minimum participation thresholds as set forth in **Appendix C. Organization HMIS Participation Agreements**. These systems may include CARES, AWARDS, and other data systems owned or operated by providers.
Project Exit	Data collection point indicating the element is required to be collected at every project exit. Elements collected at project exit must have an Information Date that matches the client's Project Exit Date.
Record	Any paper or electronic file or document that contains PII.
Record Creation	Data collection point indicating the element is required to be collected when the client record is created. Elements collected at record creation should have one and only one value for each client in an HMIS.
Universal Data Elements	Client level data elements required for collection by all projects participating in HMIS, regardless of project type or funding source; specific elements are listed in the Data Quality Plan (**Section 7. Data Quality Plan** of these policies and procedures).

Update	Data collection point indicating that the element may be collected and entered into HMIS at multiple points during an enrollment in order to track changes over time. The system must be able to support a theoretically unlimited number of update records per enrollment. Each “update” requires the creation of a new record with a distinct Information Date.

1.5. Policy Review and Amendment

Policy: The HMIS policies and procedures, including the Security Plan, Disaster Plan, and Privacy Policy, must comply with HUD regulations and/or technological changes. Updates to the policies and procedures must be reviewed and approved by the Steering Committee annually and within six months of any changes to the system management process, the data warehouse software, the methods of data exchange, or any HMIS data or technical requirements issued by HUD. The HMIS Lead is responsible for implementing the changes within six months of final approval by the Steering Committee.

Procedure: The Data Management Committee (DMC) will review the policies and procedures annually and at the time of any change to the system management process, the data warehouse software, the methods of data exchange, or any HMIS data or technical requirements issued by HUD. In the event that changes are required to the HMIS policies and procedures, the DMC will develop recommendations to the Data Management Committee for review, modification, and approval. The HMIS Team will present the Steering Committee with recommended changes to the policies and procedures, and the new policies and procedures will be reviewed, modified, and voted on by the Steering Committee and HMIS Director. The HMIS Director and DMC will modify practices, documentation, and training material to be consistent with the revised policies and procedures within six months of approval.

1.6. Data Ownership

Policy: The HMIS Lead shall manage the data that is maintained in the NYC HMIS Data Warehouse and will have access to all data entered by CHOs. The Steering and Data Management Committees will have access to aggregated and/or otherwise de-identified data that have met quality assurance standards as stipulated by HMIS Lead staff.

Procedure: The HMIS Lead has established a hierarchy of access to data for the HMIS Project.

The hierarchy begins with the client who can, at any time, submit a written request to the organization that uploaded his or her data to revoke his or her consent to provide personal information to the CHO’s project-level HMIS-compliant system and/or the Data Warehouse. If the client wishes to have the data removed from the Data Warehouse, the CHO HMIS Administrator must submit a written request to that effect to the HMIS Director. Written requests may be completed by email. All requests for data removal from the Data Warehouse that follow this protocol will be honored by the HMIS Lead.

Secondly, the CHO that enters data has the ability to request for review any data within the Data Warehouse that they have uploaded as a CHO.

Last, the HMIS Lead has ownership of the data within the Data Warehouse solely for the purposes outlined within these policies and procedures, namely:

- The aggregation of data for reporting across two or more projects at the community level;
- Monitoring and analyzing data quality and project performance; and
- Other purposes, such as grant applications, research, and education material, deemed consistent with the uses and disclosures described in the HMIS Privacy Policy in **Section 6. Privacy Policy** of these policies and procedures.

The HMIS Lead will not at any time change, distribute or delete data within CHO’s projects without the direct instruction of the CHO in question, except in the specific instances outlined in Section 6.7. and only according to the procedures outlined therein.

Though the data collected and packaged from the Data Warehouse is often published and made available for use in grants, research and educational material, all such data aggregations and analysis belong to the HMIS Lead, not the entity, CHO, or individual who may be using that data for their own purposes. Such aggregations may be shared at any time with the CCoC, HUD, or their designees for purposes of monitoring and analyzing data quality or project performance.

If a project and/or organization withdraws from the NYC CCoC, all historical data associated with that project and/or the organization will be maintained in the Data Warehouse.

2. HMIS Lead Project Administration and Management

2.1. HMIS Project Administration

Policy: The CCoC is responsible for HMIS Project oversight and implementation and for designating a HMIS Lead Agency to manage HMIS Project and Data Warehouse operations on its behalf, including entering and maintaining contracts with the HMIS software provider for the purposes of operating and overseeing the HMIS Data Warehouse. Policy decisions must be approved by the Steering Committee of the CCoC.

The HMIS Lead is not responsible for contracts between CHOs and their project-level HMIS-compliant system software providers, if such contracts exist. CHOs are responsible for ensuring any systems from which they upload data meet the minimum requirements outlined in **Section 3.3 Technical Requirements** of these policies and procedures.

2.1.1. CCoC Responsibility

Procedure: The CCoC is the lead planning group for HUD-funded efforts to end homelessness and for implementing and operating a homeless CoC system in NYC. As such, and per HUD policy, the CCoC is responsible for HMIS Project oversight and implementation, which encompasses planning, administration, software selection, managing the HMIS Data Warehouse in compliance with HMIS Standards, and reviewing and approving of all policies, procedures, and data management plans governing CHOs.

The CCoC's oversight and governance responsibilities are carried out by its Steering Committee, based on recommendations by the Data Management Committee, whose function is to provide support and recommendations to the CCoC Steering Committee based on the HMIS regulations and standards set forth by HUD and the implementation of the HMIS policies and procedures. The Data Management Committee will schedule monthly meetings unless it is determined that a meeting in a particular month is not necessary.

2.1.2. Project Management

Procedure: The CCoC has designated DSS as the HMIS Lead Agency to manage HMIS Data Warehouse operations on its behalf and to provide HMIS Project administrative functions at the direction of the CCoC, through its Steering Committee.

The HMIS Lead exercises these responsibilities as specified in these Policies and Procedures, which have been prepared at the direction of the CCoC Steering Committee. These responsibilities are contingent on continued receipt of the appropriate HUD grant funding, and are as follows:

- Governance and Reporting
- Planning and Policy Development
- Grant Administration
- System Administration
- End-User Administration
- Data Quality and Compliance Monitoring

The CoC Team under the DSS Federal Homeless Policy and Reporting Unit maintains ultimate responsibility for all administrative decisions related to the HMIS.

The current HMIS Lead MOU, posted on the NYC CCoC website http://www.nychomeless.com, contains the most complete, up-to-date description of the above-listed responsibilities of the HMIS Lead as project managers of the HMIS and the tasks described therein are incorporated into these Policies and Procedures by reference.

2.1.3. HMIS Lead Relationship with FTS

Procedure: The HMIS Lead enters into an annual contract with FTS to provide the NYC HMIS Data Warehouse, report servers and support which will enable the HMIS Lead to maintain compliance with the HUD HMIS requirements. The HMIS Lead also contracts with FTS to provide training related to the NYC HMIS.

The HMIS Lead will host weekly calls with FTS's Director of Client Services Division to coordinate management of issues related to the Data Warehouse and report server, changes to the HMIS, and progress of solutions being undertaken by FTS. The HMIS Director will keep the CoC Co-Chairs, CoC Steering Committee, and the DMC updated.

The annual contract between FTS and the HMIS Lead will be reviewed by NYC DSS CoC Team, and DSS Legal and a copy will be provided to both entities upon execution.

2.2. Data Warehouse Management Roles and Responsibilities

Policy: The HMIS Lead is responsible for the day to day operations of the HMIS Project and the Data Warehouse. All Data Warehouse End Users must be trained on appropriate use of the Data Warehouse and must sign the Data Warehouse End User Agreement in order to receive access to the system. Corrective action must be taken if a breach of said Agreement is discovered.

2.2.1. HMIS Project System Administration and Management

Procedure: The DSS HMIS Director/DSS HMIS Team is the central point of contact for matters related to the HMIS Project and the Data Warehouse. The HMIS Director serves as co-chair of the Data Management Committee. This position also liaises with FTS to ensure the Data Warehouse is functioning correctly and to make changes to the report server.

The HMIS Director/HMIS Team runs reports and monitors data quality and addresses technical issues.

2.2.2. HMIS Lead Security Officer

Per the policies and procedures in **Section 4. HMIS Security Plan**, the HMIS Lead must designate an HMIS Lead Security Officer. In order to ensure that all security-related matters are maintained in a single document for ease of review, the roles and responsibilities of the HMIS Lead Security Officer are described in **Section 4. HMIS Security Plan.** This section specifically describes the relationship of the HMIS Lead Security Officer to the other Data Warehouse management and administrative staff.

Procedure: Due to the organizational structure of DSS, the HMIS Lead Security Officer may operate under the direction of the HMIS Director/Team, or may not, depending on the individual named to fulfill these responsibilities at any given time. In cases where the HMIS Lead Security Officer does not operate under the express direction of the HMIS Director/Team, the two positions must work closely together on any HMIS security matter and the HMIS Lead Security Officer must inform the HMIS Director about any security-related action taken or recommendation made. To ensure coordination, the HMIS Lead Security Officer may not communicate directly with CHOs or FTS without the knowledge of the HMIS Director/Team, unless the HMIS Lead Security Officer is investigating an issue related to the HMIS Director/Team.

The HMIS Lead Security Officer must perform the duties outlined in these policies and procedures consistent with DSS Chief Information Officer (CIO) directives, HMIS Project administrative decisions made by the Assistant Commissioner of Research and Data Analytics and by HMIS Project policy decisions made by the CCoC Steering Committee.

2.2.3. Data Warehouse End Users (THIS SECTION ONLY APPLIES TO THE DSS CoC HMIS TEAM, AS THEY ARE THE ONLY END USERS WHO HAVE ACCESS TO/TOUCH THE DATA WAREHOUSE)

Procedure: CHO HMIS Administrators will recommend new End Users of NYC HMIS Data Warehouse to the HMIS Director/Team. CHO HMIS Administrators will recommend the user group providing only the privileges necessary for that user's work. The HMIS Director/Team will review all requests for access to the Data Warehouse to ensure access to PII is restricted to those employees who need such information to perform their official duties in connection with the administration of DSS projects.

Upon approval by the HMIS Director/Team (or designee), each new user of the Data Warehouse will be issued a username and password and assigned a user group and permissions that determine which modules/features of the NYC HMIS will be available to that user. The HMIS Director/Team (or designee) will assign the user group and privileges based on CHO HMIS Administrators' recommendations. The permission types are defined as:

- Internal Audit messages
- Project Chart Access
- Data Entry/Access
- Exception Overrides

The HMIS Director/Team will not allow access to the Data Warehouse by individuals who have not completed the following trainings:

- Training on the HMIS privacy, data collection, and security policies and procedures: these trainings will be offered by the HMIS Lead to all CHO HMIS Administrators (see also **Section 3.7 Training Requirements**); and
- Training on use of the Data Warehouse: these trainings may be offered in group or individual settings remotely or in-person and will cover all material in the Data Warehouse User Guide (Appendix A).

Existing End Users must complete the above trainings within six months of the effective date of these policies and procedures. The HMIS Coordinator will retain a log of each Data Warehouse End User, including the name, CHO, user group, and date training was completed.

Details about how to create a new user in the system and assign appropriate permissions can be found in the Data Warehouse User Guide (Appendix A).

2.2.4. Data Warehouse End User Agreements

Procedure: Any individual granted login credentials to the Data Warehouse will sign a Data Warehouse End User Agreement Form (Appendix B) indicating that he or has received the appropriate training and has read, understood and agrees to fulfill all of the obligations contained in the HMIS policies and procedures.

Each new Data Warehouse End User must have a NYC HMIS Data Warehouse User Agreement signed prior to being granted access to the system. The HMIS Team will retain the signed Data Warehouse End User Agreement (Appendix B) forms for a period of at least five years, or as long as the individual retains Data Warehouse log-in credentials.

All Data Warehouse End Users are responsible and accountable for safeguarding information assets from unauthorized modification, disclosure, and destruction. The CCoC considers unauthorized use or disclosure of HMIS information to be a serious matter and any Data Warehouse users found to be in breach of their Data Warehouse User Agreements will be subject to penalties or sanctions including:

- The loss of use or limitation on the use of HMIS and other office and technology resources;
- Adverse employment actions, including dismissal; and
- Civil and/or criminal prosecution and penalties.

The HMIS Lead is responsible for pursuing breaches of its User Agreements with appropriate DSS or CHO personnel. Users in violation of these agreements will be disciplined according to the disciplinary policies of their employers, in the event that they are CHO or DSS employees or volunteers, or according to the terms of their contracts, in the event that they are vendors or consultants.

2.3. HMIS Lead Communications

Policy: The HMIS Director/Team is responsible for relevant and timely communication with each CHO on matters related to the HMIS Project or the Data Warehouse.

Procedure: Each CHO is required to identify a CHO HMIS Administrator to serve as a single point of contact between CHO End Users and the HMIS Lead (see **Section 3.2.2 CHO HMIS Administrator** of these policies and procedures) on matters relating to HMIS. Each CHO is also required to identify a CHO HMIS Security Contact, which may be the same individual as the CHO HMIS Administrator, to liaise between CHO End Users and the HMIS Lead on matters specifically related to HMIS security (**see Section 4.2 HMIS Lead Security Officer and CHO HMIS Security Contact** of these policies and procedures). The HMIS Director/Team (or the HMIS Lead Security Officer, with the knowledge of the HMIS Director/Team will communicate with the CHO HMIS Administrator for all HMIS-related issues, including security issues. Security issues will also be communicated to the CHO HMIS Security Contact.

Communication will be via email, telephone, the NYC CCoC listserv, and at the Data Management Committee and Steering Committee meetings. In addition, the HMIS Lead posts announcements, resources and other related information on the NYC CCoC website (http://www.nychomeless.com).

CHOs should channel communication with the HMIS Lead about the HMIS (including system-wide policies and procedures, individual project-level HMIS-compliant system functionality, and data warehouse functionality) through their CHO HMIS Administrators and CHO HMIS Security Contacts, as appropriate.

2.4. Access Location

Policy: Regardless of where or how individuals access the Data Warehouse or project-level HMIS-compliant systems, these policies and procedures apply. The same privacy, security, and system access measures need to be applied at office work stations, in the field, or when connecting by remote access.

Procedure: All policies, procedures, and standards will be enforced regardless of the location of the computer or other device that collects or maintains data that will be or has been uploaded to the Data Warehouse. Because the Data Warehouse and some system-level HMIS-compliant systems are web-enabled software, users may access data from locations other than the HMIS Lead or CHO sites. If such a connection is made, the same levels of security must be applied and client confidentiality must be maintained.

2.5. CHO Grievance against HMIS Lead

Policy: CHOs will contact the HMIS Director/Team to resolve any concerns with the policies, procedures, or operations of the HMIS Project.

Procedure: The HMIS Lead is responsible for the operation of the HMIS Project and for implementing these policies and procedures. Any problems with these policies or the requirements the HMIS Lead has imposed upon a specific CHO are to be discussed with the HMIS Lead. CHOs will bring any grievances to the attention of the HMIS Lead Project System Administrator.

If these problems cannot be resolved by the HMIS Director/Team, the HMIS Director/Team will take them to the CoC Steering Committee and DSS Office of Planning and Performance Management (OPPM).

The Steering Committee shall have the final say in all matters regarding the HMIS Project.

2.6. HMIS Lead Grievance against FTS/HMIS Vendor (THIS SECTION APPLIES ONLY TO THE DSS CoC HMIS TEAM)

Policy: HMIS Lead will contact the HMIS Vendor Lead to resolve any concerns with the policies, procedures, or operations of the HMIS Project.

Procedure: The HMIS Lead is responsible for the operation of the HMIS Project and for implementing these policies and procedures. Any problems with these policies or the requirements the HMIS Vendor has imposed are to be discussed with the HMIS Lead.

If these problems cannot be resolved, the HMIS Lead will take them to the Data Management Committee, and finally to the Steering Committee.

The Steering Committee shall have the final say in all matters regarding the HMIS Project.

2.7. Client Grievance against HMIS Lead

Policy: Clients who believe that their data have been compromised by the HMIS Lead in a way that violates these policies and procedures must address the concern through the Grievance Committee of the NYC CCoC.

Procedure: Clients with a grievance against DSS as the HMIS Lead will address their concerns through the Grievance Committee of the CCoC. Individuals will submit grievances in writing to the co-chairs. The co-chairs will pass the grievance to the Grievance Committee, which will review it and make a recommendation back to the co-chairs. The co-chairs will make the final decision about the outcome and notify the individual.

The DSS Co-Chair of the NYC CCoC will recuse him/herself to avoid a conflict of interest at any hearing related to a grievance against DSS in its capacity as the HMIS Lead.

Clients with grievances against individual CHOs, or wishing to request access to their data stored in the HMIS Project, must bring these matters to the CHO with which they have the grievance or from which they wish to request data. The HMIS Lead will not manage such requests.

2.8. User Guide

Policy: The HMIS Lead is responsible for maintaining an up-to-date user guide for the Data Warehouse detailing how to complete basic upload and reporting operations.

Procedure: The HMIS Lead will ensure that the most up-to-date Data Warehouse User Guide is maintained as Appendix A of these policies and procedures.

2.9. Data Warehouse Availability

Policy: In the event of planned server downtime, the HMIS Coordinator will inform agencies as much in advance as possible in order to allow CHOs to plan their uploads accordingly.

Procedure: It is the intent of the HMIS Lead and FTS that the NYC HMIS Data Warehouse will be available 24 hours a day, 7 days a week, 52 weeks a year to incoming connections. However, no computer system achieves 100% uptime. In the event of planned server downtime, the HMIS Coordinator will inform CHOs via email in advance. In the event unplanned service interruptions, FTS will contact the HMIS Lead Project System Administrator, who will in turn contact CHO HMIS Administrators via email to inform them of the cause and expected duration of the interruption. FTS will notify the HMIS Lead Project System Administrator, who will in turn notify CHO HMIS Administrators via email, when normal service resumes.

The HMIS Coordinator will log all downtime, planned and unplanned, for purposes of system evaluation.

2.10. Data Warehouse Technical Support

Policy: The HMIS Lead is responsible for ensuring that timely technical support is available for all users of the Data Warehouse. Any technical issues with the Data Warehouse must be communicated to the HMIS Coordinator to facilitate prompt response and ensure interruptions in service can be communicated to all affected users quickly. CHO AWARDS users may also report technical challenges directly to FTS. **The HMIS Lead is not responsible for technical support of any hardware or software employed by CHOs for the purposes of their project-level HMIS-compliant systems.**

Procedure: In the event of technical issues with the Data Warehouse (i.e. not the project-level HMIS-compliant system), CHO HMIS Administrators will follow the procedures outlined below, depending on the project-level HMIS-compliant system they are operating.

<u>CHO HMIS Administrators of non-AWARDS systems</u> will contact the HMIS Coordinator by phone or email for technical support. S/he will work with CHO to resolve any issues and will forward the issue to FTS on behalf of the CHO if necessary. CHO HMIS Administrators should be prepared to share the CSV file and any other relevant information that may assist the HMIS Coordinator and/or FTS staff in resolving the issue.

CHO HMIS Administrators of AWARDS systems will follow the process for the FTS online help desk established in the Data Warehouse User Guide (Appendix A). In addition, the CHO HMIS Administrator will notify the HMIS Coordinator by email of the submission of a help desk request. The HMIS Coordinator will determine the extent to which the request must be monitored and/or the information shared with other users.

3. CHO HMIS Participation Policies

3.1. Participation Agreements and Certifications

Policy: Each CHO must execute an **Appendix C. Organization HMIS Participation Agreement** with the HMIS Lead annually. Any organization wishing to begin uploading to the Data Warehouse will have to sign the **Appendix C. Organization HMIS Participation Agreement** before it will be allowed to upload to the Data Warehouse.

The **Appendix C. Organization HMIS Participation Agreement** will cover all projects uploading data from the CHO, regardless of whether the project receives federal or other funds that require participation in HMIS or is voluntarily uploading data.

In order to be considered an HMIS participating project for purposes of HUD or other federal, state, or local agency requirements, each of the CHO's projects must:

1. Collect all data elements required for the project as specified in **Section 7. Data Quality Plan** of these policies and procedures.
2. Enter client-level data for each required data element into the project-level HMIS-compliant system within 3 business days of client interaction.
3. Complete an upload of all required data elements to the Data Warehouse within the first 10 business days of each month, as per the standards set in the **Section 7. Data Quality Plan** of these Policies & Procedures.
4. Ensure that the data uploaded to the Data Warehouse meet the data quality standards set forth in **Section 7. Data Quality Plan** of these policies and procedures.
5. Operate as a project of a CHO that is otherwise abiding by the terms of the **Appendix C. Organization HMIS Participation Agreement,** including all requirements related to privacy and security.

Procedure: Within 6 months of the effective date of these policies and procedures, and annually thereafter, the HMIS Lead will coordinate with each current CHO to develop and execute an **Appendix C. Organization HMIS Participation Agreement.** Agencies wishing to begin uploading subsequent to the effective date of these policies and procedures will work with the HMIS Lead to develop and execute **Appendix C. Organization HMIS Participation Agreement** prior to any upload to the Data Warehouse.

The terms of the **Appendix C. Organization HMIS Participation Agreement** may differ between CHOs or change over time and, as long as the recitals are consistent with these policies and procedures, they are not subject to review and approval by the CCoC Steering Committee. Each CHO will be held to the terms of the **Appendix C. Organization HMIS Participation Agreement** most recently executed by the CHO and the HMIS Lead.

Each CHO will be required to certify current or pending compliance with these policies and procedures using two certification checklists and one data collection form for each participating project that will all be incorporated into the **Appendix C. Organization HMIS Participation Agreement** by reference and compliance certified annually at the time of the execution of the Agreement. These certifications will be signed by appropriately authorized staff, as indicated on each certification form. The checklists will cover the following topics:

Administrative and Software Certification (Appendix D)

- CHO maintains a policy for granting access to its project-level HMIS-compliant systems End Users consistent with the minimum requirements set forth in **Section 3.6 CHO End Users** of these policies and procedures and is in compliance with said policies and procedures.
- CHO maintains an HMIS privacy policy consistent with the privacy standards set forth in **Section 6. Privacy Policy** of these policies and procedures and is in compliance with said policies and procedures.
- CHO's project-level HMIS-compliant system meets the technical requirements set forth in **Section 3.3. Technical Requirements** of these policies and procedures.

Security Certification Checklist (Appendix E)

CHO is in compliance with the security standards set forth in **Section 4. HMIS Security Plan**

Project Information Form (Appendix F)

One form must be completed for each participating project and updated annually.

The forms required to certify Administrative/Software compliance and Security compliance are provided in Appendix D and E, respectively. The Project Information Form is provided in Appendix F.

The HMIS Lead Agency will maintain a file of all active **Appendix C. Organization HMIS Participation Agreements** and will ensure that the certifications are updated at least annually.

3.2. Administrative Roles and Responsibilities

Policy: Each CHO must designate an Executing Officer, a CHO HMIS Administrator, and a CHO HMIS Security Contact. (One individual may fulfill more than one role). These individuals must be aware of the designation and their responsibilities in the role. Each individual fulfilling these roles must have an email address. Any changes to the name or contact information for these roles must be communicated to the HMIS Lead within 15 business days of the change. These designations must be reviewed annually through the **Appendix C. Organization HMIS Participation Agreement** certification update process.

Each CHO must maintain written documentation outlining the roles and responsibilities of these designations, consistent with these policies and procedures and its Participation Agreement, including protocols for internal communication regarding HMIS Project issues.

3.2.1. CHO Executing Officer

Procedure: Each CHO will designate the executing officer (e.g. Executive Director or Chief Executive Officer) who has authorization to execute the **Appendix C. Organization HMIS Participation Agreement**, designate the CHO HMIS Administrator and CHO HMIS Security Contact, and certify CHO compliance with these policies and procedures. This individual is expected to be an authorized signer for the CHO.

This designation will be made in the Administrative and Software Certification (Appendix D) document and will be certified annually. The CHO will provide an email address for the executing officer. Any changes to the individual assigned to serve as the Executing Officer or contact information will be communicated to HMIS Lead Project System Administrator within 15 business days of the change.

The HMIS Lead will maintain a list of all executing officer email addresses. All correspondence related to the **Appendix C. Organization HMIS Participation Agreement** will be sent to the Executing Officer.

3.2.2. CHO HMIS Administrator

Procedure: Each CHO Executing Officer will designate one staff person (which may be him or herself) and a backup to function as the NYC CHO HMIS Administrator, and this person's name and contact information will be updated annually. The designation of this individual will be made in **the Appendix D. Administrative and Software Certification Checklist**. The duties of the CHO HMIS Administrator will be included in the individual's job description or **Appendix D. Administrative and Software Certification Checklist**, and signed by the CHO HMIS Administrator to indicate understanding and acceptance of these responsibilities.

The CHO HMIS Administrator will serve as a single point of access between the End Users at the CHO and the HMIS Lead on HMIS issues. This person will be responsible for ensuring the CHO is performing quality checks on participating projects' data, errors in the data are corrected, oversight of CHO End Users, and data from each of the organization's participating projects are uploaded to the HMIS within the first ten business days of each month.

The CHO HMIS Administrator will be the channel through which the HMIS Lead will communicate information regarding updated policies and procedures, data quality performance, and other related issues. The CHO HMIS Administrator is responsible for communicating the information to his/her organization, as appropriate.

CHO HMIS Administrators will be aware of the sensitivity of client-level data and take appropriate measures to prevent its unauthorized disclosures. CHO HMIS Administrators are responsible for protecting institutional information to which they have access and for reporting security violations to the appropriate authority.

Other responsibilities of the CHO HMIS Administrator may include, but are not limited to:

- Providing a single point of communication between the End Users and the HMIS Lead around HMIS issues
- Ensuring the stability of the CHO connection to the internet and the Data Warehouse, either directly or in communication with other technical professionals
- Training CHO End Users in CHO data collection, security and privacy policies and procedures, and assuring End Users receive any requisite training provided by HMIS Lead for End Users
- Providing support for the generation of CHO reports
- Managing CHO end user licenses
- Monitoring compliance with standards of client confidentiality and data collection, entry, and retrieval
- Participating in CHO HMIS Administrators training and regular meetings

The minimum required responsibilities of the CHO HMIS Administrator will be detailed in the **Appendix C. Organization HMIS Participation Agreement**. The designation of the CHO HMIS Administrator will be made in the Administrative and Software Certification (Appendix D) document and will be reviewed annually. The CHO will provide an email address for the CHO HMIS Administrator. Any changes to the individual assigned to serve as the CHO HMIS Administrator or contact information will be communicated to HMIS Director/Team within 15 business days of the change.

The HMIS Lead will maintain a list of all CHO HMIS Administrator email addresses.

3.2.3. Security Contact

Per the policies and procedures in **Section 4. HMIS Security Plan**, each CHO will designate a CHO HMIS Security Contact. In order to ensure that all security-related matters are kept together in a single document for ease of review, the roles and responsibilities of the CHO HMIS Security Contact are described in **Section 4. HMIS Security Plan.** This section specifically describes the process of designating the Security Contact and making any updates to that designation.

Procedure: The designation of the Security Contact will be made in the Security Certification document and will be reviewed annually. The CHO must provide an email address for the Security Contact. Any changes to the individual assigned to serve as the CHO HMIS Security Contact or that individual's contact information must be communicated to HMIS Director/Team within 15 business days of the change.

The HMIS Lead will maintain a list of all CHO HMIS Security Contact email addresses.

3.2.4. CHO Communications

Procedure: Each CHO will maintain a written policy detailing its internal communication practices for HMIS matters. Minimally, the policy must state that individual CHO End Users must communicate all HMIS Project or Data Warehouse matters to the CHO HMIS Administrator and all HMIS security matters to the CHO HMIS Security Contact, in addition to the CHO HMIS Administrator. The policy must further state that the CHO HMIS Administrator is responsible for communicating to all CHO End Users any HMIS information that is relevant to the End User.

Each CHO will indicate in **Appendix D. Administrative and Software Certification Checklist** whether or not such a policy exists and has been communicated to all staff. If such a policy does not exist at the time of execution of the **Appendix C. Organization HMIS Participation Agreement**, or at the time of the annual certifications thereafter, the CHO must establish a date not later than three months from the certification date by which such a policy will be developed and implemented.

The process for communicating with the HMIS Lead is outlined in **Section 2.3 HMIS Lead Communications** of these policies and procedures.

3.3. Technical Requirements

Policy: Each CHO is responsible for maintaining a project-level HMIS-compliant system for every project required to participate in HMIS and any other project voluntarily participating in HMIS.

3.3.1. Technical Standards for Project-level HMIS-compliant Systems

Procedure: The client data collection system employed by each project uploading data to the Data Warehouse must:

- Be a relational database capable of recording client data from a limitless number of service transactions and preserving all required historical data as outlined in **Section 7. Data Quality Plan** of these policies and procedures and the HUD HMIS Data Standards in effect at the time of the adoption of these Policies and Procedures;
- Have the capacity to collect data on system use for the purposes of data quality and security, including login attempts, search parameters, and incidents of changes made to records;
- Have the capacity to collect all project descriptor, universal, and program-specific data elements as specified in **Section 7. Data Quality Plan** of these policies and procedures;
- Have the capacity to meet technical security requirements specified in **Section 4. HMIS Security Plan** of these policies and procedures and technical privacy requirements specified in **Section 6. Privacy Policy** of these policies and procedures; and
- Have the capacity to transfer data directly to the Data Warehouse or export a CSV file of all required data elements consistent with current HUD HMIS CSV Format documentation for the purposes of upload to the Data Warehouse.

Each CHO will indicate in **Appendix D. Administrative and Software Certification Checklist** whether or not its project-level system meets all of the above requirements. If the system does not meet each of these requirements at the time of execution of the **Appendix C. Organization HMIS Participation Agreement**, or at the time of the annual certifications thereafter, the CHO must establish a date not later than three months from the certification date by which each instance of non-compliance will be resolved. An updated **Appendix D. Administrative and Software Certification Checklist** form indicating full compliance must be provided to the HMIS Lead by the target date or the CHO will be considered to be in violation of the terms of the **Appendix C. Organization HMIS Participation Agreement**.

The HMIS Lead is not responsible for technical support of any hardware or software employed by CHOs for the purposes of their project-level HMIS-compliant systems.

3.3.2. Data Upload Hardware/Software requirements

Procedure: Once a CHO project is set up in the Data Warehouse (according to the procedures described in **Section 3.4 CHO and Project Activation** of these policies and procedures), all that is needed to upload to the Data Warehouse is an internet connection. Any provider not using AWARDS must be able to create CSV files according to HUD's specifications.

In order for the HMIS Lead to maintain awareness of any technical issues affecting CHOs, CHOs must communicate any Data Warehouse issues to the HMIS Coordinator, according to the procedures specified in **Section 2.9 Data Warehouse Technical Support** of these policies and procedures within 3 business days of the onset of the issues.

3.4. CHO and Project Activation

Policy: Once the HMIS Lead has received a completed **Appendix C. Organization HMIS Participation Agreement** and all required certifications as specified in **Section 3.1 Participation Agreements and Certifications** of these policies and procedures, the HMIS Lead will set up new CHOs and projects in the Data Warehouse and create a username for the CHO HMIS Administrator, if needed.

Procedure: CHOs that are already participating in the NYC HMIS and want to add a project must notify the HMIS Lead. In order to set up a new project for new and existing CHOs, the following steps will be taken:

1. The CHO will complete the Project Information Form, Appendix F to these policies and procedures, to provide all relevant program descriptor data elements and request implementation.
2. The CHO will work with the HMIS Coordinator to review Appendix F, data quality and confirm that the project is ready to upload data.
3. The CHO will set up the project in AWARDS. For new projects, the HMIS project name must match the project name in the HUD, HPD, OTDA, OASAS, OMH, DHS, DSS or other funder contract. The setup will be reviewed by the HMIS Coordinator prior to the initial upload.

CHOs must not upload new projects to the NYC HMIS without prior approval from the HMIS Coordinator.

During the first quarter of a new project's activation, the project will be in a probationary period. During this period, if it fails to meet the requirement to complete monthly uploads or to meet the data quality standards outlined in **Section 7. Data Quality Plan** of these policies and procedures it will not be considered in violation of the **Appendix C. Organization HMIS Participation Agreement** because the CCoC recognizes that a new CHO may require some time to comply with these requirements. All data quality standards for the first quarter of data must be met by the conclusion of the first quarter.

3.5. Project Naming Requirements

Policy: All organizations and projects in the Data Warehouse will be named in a consistent and standardized manner.

Procedure: For new projects, the HMIS project name must match the project name in the HUD, HPD, OASAS, OTDA, OMH, DHS or other funder contract. The suggested naming convention is "CHO Name_ProjectName_Funding Source".

3.6. CHO End Users

Policy: Each CHO must determine which of its employees need access to the project-level HMIS-compliant system. CHOs may establish user levels as they wish, so long as the levels include a distinction between an End User and an Administrative User, who has permissions to create new users, change permissions, or modify the user interface for the project-level HMIS-compliant system. End Users must sign End User agreements before being granted access to the project-level HMIS compliant system, and Data Warehouse End Users must also sign a Data Warehouse End User Agreement (Appendix B) in order to receive access to the NYC HMIS. Corrective action will be taken when a breach of said Agreement is discovered.

3.6.1. User Levels and Activation

Procedure: Each CHO will maintain a written policy detailing its management control over access authorization, user levels, and process for activating a new user. The CHO HMIS Administrator must be an administrative user.

CHO HMIS Administrators will assign user levels and activate new users only when they have signed a CHO User Agreement as specified in Section **3.6.2 CHO User Agreement** of these policies and procedures and have completed all required training for their user level as specified in **Section 3.7 Training Requirements** of these policies and procedures.

Each CHO will indicate in the Administrative and Software Certification (Appendix D) whether or not such a policy exists. If such a policy does not exist at the time of execution of the **Appendix C. Organization HMIS Participation Agreement**, or at the time of the annual certifications thereafter, the CHO must establish a date not later than three months from the certification date by which such a policy will be developed and implemented. A copy of the policy must be available to the HMIS Lead by the target date or the CHO will be considered to be in violation of the terms of the **Appendix C. Organization HMIS Participation Agreement**.

3.6.2. CHO End User Agreement

Procedure: Prior to being granted access to any project-level HMIS-compliant system, each new End User must sign a CHO End User Agreement indicating that he or she has received all required HMIS training (see **Section 3.7 Training Requirements**) and has read, understood and agrees to fulfill all of the obligations contained in these policies and procedures. Within six months of the effective date of these policies and procedures, all existing users must sign a CHO End User Agreement. An example of such an End User Agreement is provided in **Appendix G. Example NYC HMIS Project End User Agreement.** CHOs may modify the example End User Agreement to include additional user requirements relevant to their specific system or operations, as long as the provisions do not conflict with or omit any of the provisions of the example End User Agreement.

Each CHO HMIS Administrator will be responsible for the distribution, collection and storage of signed CHO End User Agreements. The signed CHO End User Agreements are subject to inspection at any time by the CCoC, through the HMIS Lead or Data Management Committee.

Each CHO will indicate in the **Appendix D. Administrative and Software Certification Checklist** whether or not such a CHO End User Agreement exists, whether or not all users have signed the Agreement, and to make available an unsigned sample copy of the Agreement (unless the CHO has adopted the example End User Agreement). If such an Agreement does not exist or not all current users have signed the Agreement at the time of execution of the **Appendix C. Organization HMIS Participation Agreement**, or at the time of the annual certifications thereafter, the CHO must establish a date not later than three months from the certification date by which an appropriate CHO End User Agreement will be developed and implemented. An unsigned sample copy of the CHO End User Agreement and an updated **Appendix D. Administrative and Software Certification Checklist** form indicating full compliance must be provided to the HMIS Lead by the target date or the CHO will be considered to be in violation of the terms of the **Appendix C. Organization HMIS Participation Agreement**.

3.6.3. CHO End User Agreement Breach

Procedure: A user who breaches the terms of the CHO End User Agreement will face the sanctions specified by his/her CHO. However, any breaches related to security or privacy must be reported to the HMIS Lead within 3 business days of discovery. These breaches will be dealt with on a case by case basis. Penalties may include, but are not limited to, temporary or permanent ban from using project-level HMIS-compliant system and legal action.

Each CHO will develop and implement a written policy for managing a breach of the User Agreement. The CHO HMIS Administrator should use all reasonable measures to ensure staff complies with these policies and procedures. At minimum, CHOs will inform users that unauthorized use or disclosure of PII is considered a serious matter and will result in penalties or sanctions, which may include:

- The loss of use or limitation on the use of the project-level HMIS-compliant system and other office and technology resources;
- Financial liability for the cost of such use;
- Adverse employment actions including dismissal; and
- Civil and/or criminal prosecution and penalties.

Each CHO will indicate in the **Appendix D. Administrative and Software Certification Checklist** whether or not such a policy exists. If such a policy does not exist at the time of execution of the **Appendix C. Organization HMIS Participation Agreement**, or at the time of the annual certifications thereafter, the CHO must establish a date not later than three months from the certification date by which such a policy will be developed and implemented. A copy of the policy must available to the HMIS Lead by the target date or the CHO will be considered to be in violation of the terms of the **Appendix C. Organization HMIS Participation Agreement**.

3.7. Training Requirements

Policy: Each CHO is responsible for ensuring all End Users are appropriately trained on system use, privacy, security, and data collection requirements. The HMIS Lead will provide training to CHO HMIS Administrators and Security Contacts to ensure they are adequately trained to provide such trainings to their End Users. At the discretion of the HMIS Lead, additional trainings may be offered to CHO HMIS Administrators, Security Contacts, and other users.

Procedure: Each CHO will develop and implement appropriate training for all End Users on system use, privacy, security, and data collection requirements. To support this, the HMIS Lead will offer trainings and train-the-trainer sessions to all CHO HMIS Administrators and Security Contacts initially, prior to executing the **Appendix C. Organization HMIS Participation Agreement** and annually or as needed to review updates, changes, or to refresh users. The HMIS Lead may conduct additional trainings at its discretion.

At minimum, the trainings offered by the HMIS Lead will cover:

- Train-the-trainer on HMIS Basics: Privacy, security and data collection requirements as set forth in these policies and procedures
- HMIS for Administrators: Managing data quality and project performance management using HMIS
- HMIS for Security Contacts: In-depth security training

Other End Users may attend these sessions at the discretion of the HMIS Lead as outlined in the **Appendix C. Organization HMIS Participation Agreement**.

Each CHO is responsible for training all End Users on the use of its project-level HMIS-compliant system before the user is authorized to collect and enter data in the project-level HMIS-compliant system for upload to the Data Warehouse.

Each CHO will indicate in **the Appendix D. Administrative and Software Certification Checklist** whether or not each End User has received appropriate training on system use, privacy, security, and data collection requirements consistent with the train-the-trainer sessions provided by the HMIS Lead and these policies and procedures. If this has not occurred at the time of execution of the **Appendix C. Organization HMIS Participation Agreement**, or at the time of the annual certifications thereafter, the CHO must establish a date not later than three months from the certification date by which these trainings will be completed. An updated **Appendix D. Administrative and Software Certification Checklist** form indicating full compliance must be provided to the HMIS Lead by the target date or the CHO will be considered to be in violation of the terms of the **Appendix C. Organization HMIS Participation Agreement**.

3.8. Compliance

Policy: The HMIS Lead and CHOs must communicate frequently to ensure that requirements and obligations established in the **Appendix C. Organization HMIS Participation Agreement** are being met. Projects that demonstrate persistent non-compliance and do not demonstrate good faith efforts to resolve challenges will have their project participation suspended or terminated by the HMIS Lead according to the terms specified in the **Appendix C. Organization HMIS Participation Agreement**.

In the event of termination of project from the HMIS or the termination of the **Appendix C. Organization HMIS Participation Agreement** by either party, the project (or organization) will no longer be permitted to upload data to the HMIS. It will cease to be considered an HMIS participant for purposes of HUD or other federal, state, or local agency requirements. This may affect contractual relationships requiring participation in HMIS. All data entered into the Data Warehouse will remain an active part of the Data Warehouse.

3.8.1. Monitoring

Procedure: Monitoring of compliance with the terms of **the Appendix C. Organization HMIS Participation Agreement** and these policies and procedures is the responsibility of the HMIS Lead. The HMIS Lead will use the following mechanisms to complete this monitoring:

- Data quality reports as outlined in **Section 7. Data Quality Plan** of these policies and procedures to verify that all required data elements are being collected by the CHO and uploaded with the required frequency;
- Annual certifications, incorporated into **Appendix C. Organization HMIS Participation Agreement**, demonstrating that all End Users have signed an appropriate User Agreement, and that the organization maintains all policies and processes needed to meet all participation requirements; and

- At the discretion of the HMIS Lead and CCoC Data Management Committee can request a meeting with a CHO to review: data quality issues, uploads, policies and processes needed to meet all participation requirements, and document reviews.

CHOs are encouraged to communicate frequently with the HMIS Lead to reconcile reports coming from the Data Warehouse and from the project-level HMIS-compliant system. CHOs that are working to reconcile their policies with the requirements outlined in the certification documents are also encouraged to communicate frequently with the HMIS Lead as they make necessary corrections. Addressing issues as they arise will allow time for them to be fixed or for training or technical assistance to be provided well in advance of any reporting or certification deadline.

3.8.2. Contract Terminations Initiated by the CHO

Procedure: CHOs no longer wishing to participate in the NYC HMIS, in whole or for a specific project, must submit a letter to the HMIS Lead stating this intention and the effective date when participation will stop. The HMIS Lead will deactivate all relevant Data Warehouse users from that CHO on the specified date. All historical data entered into the Data Warehouse by that CHO or project will be maintained in the Data Warehouse. A CHO withdrawing from the HMIS may request an export of its data in CSV format.

If the project is required to participate in HMIS, the HMIS Lead will notify the Data Management Committee and the Steering Committee of the change in status. Projects for which there is no current, applicable **Appendix C. Organization HMIS Participation Agreement** will be subject to deductions during the annual project evaluation process and may be denied inclusion in the CCoC's application for HUD CoC Program funding.

In the event that the HMIS Lead discovers that a CHO or a specific project has ceased operations (i.e. clients are no longer receiving services through a specific project or any project of the organization) without notifying the NYC HMIS Lead and/or updating the status of its clients through a final upload to the Data Warehouse, the HMIS Lead will notify the HMIS Data Management Committee and the Steering Committee. Upon approval from the Steering Committee, the HMIS Lead will close all client records that were open at the time of the most recent upload by that CHO or project.

3.8.3. Contract Terminations of CHO Initiated by the HMIS Lead

Any CHO found to be in violation of the terms of the **Appendix C. Organization HMIS Participation Agreement** will be notified of this status in writing. Correspondence on this matter will be addressed to the CHO Executive Director and all such correspondence will be reported to the Data Management Committee. If violations cannot be resolved within 90 days of the date of this correspondence, the HMIS Lead may terminate the **Appendix C. Organization HMIS Participation Agreement**.

CHOs who dispute the HMIS Lead's assessment of compliance must submit a grievance through the Grievance Committee. In the event that resolution of a grievance extends beyond the 90-day window in which the CHO must resolve its violations, the Grievance Committee will extend the window until the Grievance Committee delivers a decision.

In the event that the **Appendix C. Organization HMIS Participation Agreement** or a project within a CHO is to be terminated, the HMIS Lead will provide up to 30 days written notice to the CHO's Executive Director. The HMIS Lead may require that the CHO or project rectify any outstanding upload or client status matters before the termination is final and will inactivate all applicable Data Warehouse users from that CHO on the specified date. All historical data entered into the Data Warehouse by that CHO will be maintained in the Data Warehouse.

If the project is required to participate in HMIS, the HMIS Lead will notify the Data Management Committee and Steering Committee of the change in status. Projects for which there is no current, applicable **Appendix C. Organization HMIS Participation Agreement** will be subject to deductions in the annual project evaluation process and may be denied inclusion in the CCoC's application for HUD CoC Program funding.

3.8.4 Contract Terminations of FTS/HMIS Vendor Initiated by the HMIS Lead

Any HMIS Vendor found to be in violation of the terms of the **Appendix C. Organization HMIS Participation Agreement** will be notified of this status in writing. Correspondence on this matter will be addressed to the HMIS Vendor Executive Director and all such correspondence will be reported to the Data Management Committee. If violations cannot be resolved within 90 days of the date of this correspondence, the HMIS Lead may terminate the **Appendix C. Organization HMIS Participation Agreement**.

The HMIS Vendor who disputes the HMIS Lead's assessment of compliance must submit a grievance through the Grievance Committee. In the event that resolution of a grievance extends beyond the 90-day window in which the HMIS Vendor must resolve its violations, the Grievance Committee will extend the window until the Grievance Committee delivers a decision.

In the event that the **Appendix C. Organization HMIS Participation Agreement** with the HMIS Vendor is to be terminated, the HMIS Lead will provide up to 30 days written notice to the HMIS Vendor's Executive Director. The HMIS Lead may require that the HMIS Vendor or project rectify any outstanding uploads, reports, or client status matters before the termination is final and will inform all CHO Users that the HMIS System is being terminated on the specified date. All historical data entered into the Data Warehouse will be maintained in the Data Warehouse.

The HMIS Lead will notify all CHOs, the Data Management Committee, and Steering Committee of the change in status.

4. HMIS Security Plan

4.1 Goal and Purposes

The goal of the HMIS Security Policies and Procedures ("HMIS Security Plan") is to ensure that HMIS data are collected, used, and maintained in a confidential and secure environment at all times. The boundaries of the HMIS implementation are described in **Section 1. HMIS Overview** of these policies and procedures. The Security Plan applies to the HMIS Lead, the Data Warehouse, CHOs, and their project-level HMIS-compliant systems. Specific applicability is described in each policy within this security plan. This Plan applies to all Personally Identifiable Information (PII) collected for inclusion in the Data Warehouse or a project-level HMIS-compliant system or generated from the same, regardless of whether or not that data has been entered or uploaded into these systems and regardless of the format of the data (electronic or hard copy).

The NYC CCoC recognizes that agencies may have established their own security policies that meet the HUD security requirements and minimum standards set forth below. One purpose of this document is to outline those standards to all CHOs and define the parameters of compliance with these standards. The document is not intended to supplant individual CHO security policies. As long as CHO policies and practices meet the minimum thresholds established in this plan, they may establish additional or more stringent security requirements for their project-level HMIS-compliant system. The other purpose of this document is to describe how the HMIS Lead and the Data Warehouse meet security requirements established in HUD's security standards.

4.2 HMIS Lead Security Officer and CHO Security Contact Roles and Responsibilities

Policy: The HMIS Lead must designate an NYC HMIS Security Officer. Each CHO must designate a NYC HMIS Security Contact who is responsible for ensuring each CHO is meeting the minimum security requirements established in the HMIS Security Plan and the **Appendix C. Organization HMIS Participation Agreement**, and is authorized by the Executing Officer of the CHO to provide verification of that status.

HMIS Lead Procedure: The HMIS Lead Security Officer is named in the HMIS Lead Security Certification checklist which must be updated at least annually. The contact information is incorporated into this Security Plan by reference. The duties of the HMIS Security Officer must be included in the individual's job description or HMIS Lead Security Certification, and signed by the HMIS Security Officer to indicate understanding and acceptance of these responsibilities. These duties include, but may not be limited to:

- Cooperatively with the HMIS Director/Team, review the HMIS Security Plan annually and at the time of any change to the security management process, the data warehouse software, the methods of data exchange, and any HMIS data or technical requirements issued by HUD. In the event that changes are required to the

HMIS Security Plan, work with the HMIS Director/Team to develop recommendations to the Data Management Committee for review, modification, and approval.

- Annually review the HMIS Lead Security Certification document, test the HMIS Lead security practices for compliance, and work with the HMIS Director/Team to coordinate communication with FTS to confirm security compliance of the Data Warehouse.
- Using the HMIS Lead Security Certification document, certify that the HMIS Lead adheres to the Security Plan or develop a plan for mitigating any shortfall, including milestones to demonstrate elimination of the shortfall over as short a period of time as is possible.
- Implement any approved plan for mitigation of shortfalls and provide appropriate updates on progress to the Steering Committee.
- Respond, in cooperation with the CHO HMIS Administrator, to any security questions, requests, or security breaches to the HMIS Director/Team and HMIS Lead Security Officer, and for communicating security-related HMIS information relayed from HMIS Lead to the CHO's HMIS Security Contact.

CHO Procedure: Each CHO will provide the name and contact information of the CHO HMIS Security Contact at least annually in **Appendix E. Security Certification Checklist**. Changes to the individual named as the Security Contact that occur during the course of the year will be communicated via email to the HMIS Director/Team and HMIS Lead Security Officer within fifteen business days of the change.

The HMIS Lead will maintain the name and contact information of the current Security Contact of each CHO on file. This file is considered part of the HMIS Security Plan and is incorporated by reference.

The duties of the Security Contact are included on **Appendix E. Security Certification Checklist**, and signed by the Security Contact to indicate understanding and acceptance of these responsibilities. These duties include, but may not be limited to:

- Annually review the **Appendix E. Security Certification Checklist**, test the CHO security practices for compliance, and work with appropriate vendors (where applicable) to confirm security compliance of the project-level HMIS-compliant system.
- Using the **Appendix E. Security Certification Checklist**, certify that the CHO adheres to the HMIS Security Plan or provide a plan for mitigating any shortfall, including milestones to demonstrate elimination of the shortfall over time.
- Communicate any security questions, requests, or security breaches to the HMIS Director/Team and HMIS Lead Security Officer, and security-related HMIS information relayed from HMIS Lead to the CHO's End Users.
- Complete security training offered by the HMIS Lead.

Additional duties that may be incorporated in the **Appendix C. Organization HMIS Participation Agreement** on a case-by-case basis include:

- Provide security training to CHO's End Users based on Security training provided to the CHO HMIS Security Contact by the HMIS Lead.

Any security-related questions from CHO staff will be communicated to the HMIS Lead via the CHO HMIS Security Contact, consistent with **Section 2.3 HMIS Lead Communications** of these policies and procedures.

4.3 Compliance Review

Policy: The HMIS Lead is responsible for ensuring that the HMIS implementation is operated in accordance with HUD standards. The HMIS Lead is responsible for conducting a security review of the Data Warehouse annually and reporting any issues to the Steering Committee. Each CHO is responsible for conducting a security review annually and certifying that each participating project is in compliance with the NYC HMIS Security Plan and HUD standards. The CCoC, through the Data Management Committee or the HMIS Lead Agency, retains the right to conduct site visits to check compliance with the security policies and procedures and to verify self-certification of the CHOs.

HMIS Lead Procedure: The HMIS Lead Security Officer will test the HMIS Lead security practices and complete the HMIS Lead Security Certification document annually. The form will be submitted to the Data Management Committee for review. In the event that any items reviewed are not implemented in compliance with this Security Plan, the Data Management Committee must review and approve the HMIS Lead's plan for mitigating the shortfall, including benchmarks to demonstrate elimination of the shortfall over time. The Steering Committee is responsible for continued oversight of the HMIS Lead's alignment with the Security Plan.

CHO Procedure: Each CHO's Security Contact will be responsible for testing its security practices and completing the Security Certification document annually. This document is provided in **Appendix E. Security Certification Checklist.** This form will be included as **Appendix C. Organization HMIS Participation Agreement** (see **Section 3. CHO HMIS Participation Policies** of these policies and procedures). Failure to submit this form within 30 days of its due date in any given year will, like any violation of these policies and procedures, require the organization to undergo graduated sanctions that may render the organization ineligible to receive HMIS reimbursement for that year and could include loss of funding.

Each CHO will indicate in the Security Certification whether or not it meets each of the requirements outlined in the Security Plan. If a requirement is not met at the time of execution of the **Appendix C. Organization HMIS Participation Agreement**, or at the time of the annual certifications thereafter, the CHO must establish a date not later than three months from the certification date by which that requirement will be met. An updated Security Certification document indicating full compliance will be provided to the HMIS Lead by the target date or the CHO will be considered to be in violation of the terms of the **Appendix C. Organization HMIS Participation Agreement** and will be subject to the procedures described in **Section 3.8.3 Contract Terminations Initiated by the HMIS Lead** of these policies and procedures

4.4 Use Requirements

Policy: The CCoC recognizes the sensitivity of the data in the NYC HMIS Data Warehouse, and therefore requires that the individuals responsible for managing the HMIS be subject to criminal background checks and that each End User of the Data Warehouse or any project-level HMIS-compliant system be adequately trained in security measures, appropriate to his or her access level.

4.4.1 Criminal Background Verification

HMIS Lead Procedure: The HMIS Lead Security Officer and any user able to access data from more than one CHO will undergo criminal background verification. Record of the completed background check (though not the results) are subject to inspection by the CCoC.

The HMIS Lead will hire individuals with criminal justice histories only to the extent the hire is consistent with any relevant hiring policies of DSS, unless the background check reveals a history of crimes related to identity theft or fraud. The HMIS Lead will manage the results of any background checks conducted on a case by case basis.

CHO Procedure: As long as they comply with all relevant laws, CHOs will follow their own policies regarding conducting background checks and hiring individuals with criminal justice histories.

4.4.2 Annual Security Training

HMIS Lead Procedure: As described in **Section 2.2.3 Data Warehouse End Users** of these policies and procedures, the HMIS Director/Team will document that each End User of the Data Warehouse has completed security training provided by the HMIS Lead prior to gaining system access and at least annually thereafter.

CHO Procedure: As described in **Section 3.6 CHO End Users** of these policies and procedures, the CHO Security Contact (or other appropriate individual) will document that each End User of that CHO has completed security training prior to gaining system access and at least annually thereafter. This training, at minimum, must meet the requirements outlined in the HMIS Lead's Train-the-Trainer Security sessions.

4.5 Data Warehouse Security

Policy: The HMIS Lead is responsible for ensuring that the Data Warehouse is operated securely. The HMIS Lead will take all possible measures to ensure that the Data Warehouse is protected from intrusion and data loss. End Users of the Data Warehouse are responsible for understanding security-related requirements, are prohibited from sharing their username or password with any other individual, and are required to maintain the security and confidentiality of HMIS data in any format.

4.5.1 Physical Security

Procedure: The HMIS Lead will include provisions in its contract with FTS requiring FTS to protect the physical security of the facilities and media in which the data is stored. FTS will use two data centers in two different states on four different power grids to host the HMIS data. These data centers feature uninterruptible power supplies and sophisticated disaster prevention and recovery systems. Biometric confirmation of identity is required to enter the data centers. The data centers feature porous floors to prevent flood damage, "dry" sprinkler pipes, fire suppression gas instead of water, a diesel generator that picks up immediately in the advent of a power failure, industrial air filtering and air conditioning technologies, and a live 24-hour armed guard. The main data center is run by Verizon (formerly MCI), while the backup data center is maintained by Datapipe.

In the data centers, FTS will use servers with multiple hard drives (RAID 5), CPUs, and redundant power supplies so that if any internal components malfunction, there is immediate failover with minimal interruption in service.

4.5.2 Backup

Procedure: The HMIS Lead will include provisions in its contract with FTS requiring FTS to maintain backup versions of the data stored in the Data Warehouse at a separate physical location consistent with the most up-to-date HUD HMIS technical and security standards. FTS will back up all data on multiple servers in multiple locations and on multiple power grids three times per day and at the end of each day. FTS will be moving toward a LivePoint In Time backup system to be in place by April 1, 2018. FTS will also perform weekly and monthly data backups. All backups will be held offsite at a secondary data center, except the intra-day and daily backups, which will be held on a local server as well as offsite at the secondary data center. All data will be copied to a second server so that if an entire server malfunctions, data will be available immediately with no service interruption. The failover function will be tested at least once per year and after each major system upgrade. All data storage resides on a SAN (Storage Area Network). This stored data can be presented to alternate systems as needed. This provides a layer of protection from server failure.

4.5.3 Software Security

Procedure: The HMIS Lead will include provisions in its contract with FTS requiring FTS to maintain the Data Warehouse software consistent with the most up-to-date HUD HMIS technical and security standards. FTS must retain a log of system changes and/or software version changes.

Users identifying software issues that may compromise the security of the Data Warehouse will notify the CHO HMIS System Administrator. The CHO HMIS System Administrator will work with the FTS HelpDesk. The FTS HelpDesk team will work with the application developers to address all reported bugs within forty-eight hours. If customer intervention is required, the HMIS Lead is responsible for ensuring that all FTS-released enhancements, upgrades and bug fixes are applied promptly upon release.

All -owned devices (workstations, laptops, and other systems that process and/or store PII) used to access the Data Warehouse are protected by commercial, anti-virus and Internet Security Software solutions, including but not limited to firewalls, malware, intrusion detection, etc. These solutions must be updated at least monthly or when new versions or releases become available and current security, software, or operating system patches must be applied to the computers of End Users. CHOs accessing the Data Warehouse to upload data will document procedures in their Security Policies to ensure that CHO-owned devices used to access the Data Warehouse are similarly protected by the measures listed above.

4.5.4 Boundary Protection

Procedure: The HMIS Lead will include provisions in its contract with FTS requiring FTS to take reasonable steps, consistent with the most current HUD HMIS technical and security standards, to prevent unauthorized access to the data and the software. FTS servers on which the HMIS data is stored make use of firewalls in both hardware and software form.

All -owned devices used to access the Data Warehouse are protected by a firewall between the workstation and any system, including the internet, outside DSS. CHOs accessing the Data Warehouse to upload data will document procedures in their Security Policies to ensure that CHO-owned devices used to access the Data Warehouse are similarly protected by a firewall.

4.5.5 System Access User Authentication and Passwords

Procedure: The HMIS Lead will include provisions in its contract with FTS requiring FTS to maintain access control mechanisms designed to reduce the risk of access to the data warehouse by unauthorized users. Access to the Data Warehouse is governed by multiple layers of securities – passwords, user group assignment and permissions.

All users will be given a unique username and password to log into the Data Warehouse. Default passwords must be changed upon the initial login. Passwords must be at least 8 characters and must contain at least one upper case letter, at least one lower case letter, and at least one alphanumeric character and at least one character which is numeric or a special character. Passwords must not be composed of easily guessed words, such as a user's own user ID, proper names (such as the user, application, or vendor name), or other criteria that can be associated to the user, or any of those spelled backwards. Users should not select passwords that contain personally identifiable numbers such as their phone extension, Social Security Number or home zip code. The system will automatically require each user to change his or her password at least every 90 days to a new password that is not the same as his or her previous four (4) passwords, and password cannot be changed more than once per day. Users shall not share their passwords. Writing down passwords is strongly discouraged. Passwords that are written should be appropriately stored to prevent disclosure to anyone other than the individual user. Passwords that are written should not reference the account or data store they protect.

The Data Warehouse has been set up to provide the following safeguards against access by unauthorized users:

- Requires users to log in
- FTS will prohibit users from logging in to the Data Warehouse from multiple locations simultaneously.
- Data Warehouse users will be automatically logged off of the system after 90 minutes of inactivity. The user will be required to re-enter their username and password to regain access to the system.
- In the event that a Data Warehouse End User forgets his or her password, users cannot retrieve forgotten passwords as they are not stored in the system but must instead create a new password with the assistance of the HMIS Director or HMIS Coordinator. Users can change passwords on their own.
- 10 consecutive unsuccessful login attempts will cause the system to disable the username and to notify the HMIS Director/Team of the lockout via internal messaging.

The HMIS Lead will provide unique usernames to each End User of the Data Warehouse in accordance with the procedures outlined in **Section 2.2.3 Data Warehouse End Users** of these policies and procedures. Data Warehouse End Users will be required to complete the Data Warehouse End User Agreement (Appendix B), acknowledging that they are required to maintain their passwords securely and that passwords may not be shared, even among other authorized Data Warehouse End Users.

Data Warehouse End Users may access the Data Warehouse only from computers and systems meeting all requirements established in these policies and procedures.

4.5.6 Audit Controls

Procedure: FTS maintains an accessible audit trail within the Data Warehouse that allows the HMIS Director/Team to monitor user activity. Activity will be monitored by FTS and potential or actual security incidents will reported as described in **Section 4.8 Security Incidents** of these policies and procedures. Additionally, the HMIS Director/Team will monitor audit reports monthly for any apparent security breaches or behavior inconsistent with the **Section 6. Privacy Policy** of these policies and procedures. Audit controls will include the following

a. Are capable of recording data access for specified users when requested by authorized management personnel;
b. Retain 'Read Only" Audit trail logs for five years

4.6 CHO Project-level HMIS-compliant System Security Policy

Policy: Each CHO is responsible for developing security policies and procedures for their project-level HMIS-compliant software system consistent with the requirements outlined below and in HUD standards. The HMIS Lead is responsible for monitoring the CHO-level policies and procedures as described in **Section 4.4 Use Requirements** of these policies and procedures.

4.6.1 Physical Security

Procedure: Each CHO will maintain and follow procedures protecting the physical security of the facilities and media in which the data is stored or include provisions in its contract with the provider of the project-level HMIS-compliant system to do so. At minimum, the procedures or provisions must specify that the data will be stored in a facility with appropriate temperature control and fire suppression systems. Surge suppressors must be used to protect systems used for collecting and storing all the HMIS data.

4.6.2 Backup

Procedure: Each CHO will maintain and follow procedures to copy all HMIS data on a regular basis to another medium and store it in a secure off-site location where the required privacy and security standards would also apply, or include provisions in its contract with the provider of the project-level HMIS-compliant system to do so. At minimum, the procedures or provisions must specify that the data will be backed up weekly and that the backup restoration process will be tested at least once per year.

4.6.3 Software Security

Procedure: Each CHO will maintain and follow procedures to maintain the project-level HMIS-compliant system software consistent with the most up-to-date HUD HMIS technical and security standards or include provisions in its contract with the provider of the project-level HMIS-compliant system to do so.

At minimum, these procedures or provisions must specify how the software provider or system operator will address all reported bugs within three business days and specify that, if customer intervention is required, the CHO is responsible for ensuring that all enhancements, upgrades and bug fixes are applied promptly upon release by the software provider.

In addition, each CHO will maintain and follow procedures to install, update and use anti-virus software on all CHO-owned devices used to access the project-level HMIS-compliant system. At minimum, these procedures must identify the anti-virus software in use, specify that the CHO Security Contact is responsible for managing the software, and specify the frequency with which the software will be updated and the frequency with which the devices will be scanned. CHOs must, at minimum, update the software and scan the relevant devices for viruses and malware monthly. These solutions must be updated at least monthly or when new versions or releases become available and current security, software, or operating system patches must be applied to the computers of CHO End Users. If applicable, the virus protection software must automatically scan files as they are accessed by users on the system where the HMIS application is housed.

4.6.4 Boundary Protection

Procedure: Each CHO will maintain and follow procedures for protecting HMIS data behind a firewall. If applicable, the CHO will include provisions in its contract with the provider of the project-level HMIS-compliant system to maintain a firewall between the server(s) on which any HMIS data is stored and any external systems. In addition, each CHO must protect all CHO-owned devices used to access or store HMIS data with a firewall between the device and any system, including the internet, outside the CHO.

4.6.5 System Access User Authentication and Passwords

Procedure: CHO End Users will be notified via the CHO User Agreement (see **Section 3.6.2 CHO User Agreements)** of these policies and procedures) that HMIS passwords (either to the Data Warehouse or the project-level HMIS-compliant system) may not be shared, even among other authorized CHO End Users.

Each CHO will set up their project-level HMIS-compliant system to accommodate the following requirements for passwords: All users will be given a unique username and password. Default passwords must be changed upon the initial login. Passwords must be at least 8 characters and must contain at least one alphanumeric character and at least one character which is numeric or a special character. Passwords must not be composed of easily guessed words, such as a user's own user ID, proper names (such as the user, application, or vendor name), or other criteria that can be associated to the user, or any of those spelled backwards. Users should not select passwords that contain personally identifiable numbers such as their phone extension, Social Security Number or home zip code. The system will automatically require each user to change his or her password at least every 90 days to a new password that is not the same as his or her previous four (4) passwords, and password cannot be changed more than once per day. Users shall not share their passwords. Writing down passwords is strongly discouraged. Passwords that are written should be appropriately stored to prevent disclosure to anyone other than the individual user. Passwords that are written should not reference the account or data store they protect.

Each CHO will set up their project-level HMIS-compliant system to prevent users from being able to log on to the system from more than one workstation at a time.

Each CHO will maintain and follow procedures to provide and maintain unique usernames to each new user of their project-level HMIS-compliant system. At minimum, this procedure must:

- Require users to log-into systems;
- Define a period of inactivity after which the user's workstation must be automatically logged out of the system and/or locked out of the computer, requiring a username and password to resume use of the project-level HMIS-compliant system;
- Require that any default passwords provided for initial entry into the application be changed on first use;
- Define how individual users' forgotten passwords will be reset and communicated to the user; and
- Specify how unsuccessful login attempts will be handled and confirm that the project-level HMIS-compliant system will maintain an auditable record of all attempted logins. At maximum, 5 consecutive unsuccessful login attempts must lock a user out of the system for at least 30 minutes. CHO HMIS Administrators may manually restore access prior to end of the 30 minute period.

Each CHO will maintain and follow procedures for accessing its project-level HMIS-compliant system through networks and devices not owned or managed by the CHO. At minimum, the procedures must specify that any user granted remote access will be monitored, specify that a list of such users will be maintained by the CHO, and describe how the CHO will ensure the security of the system and the confidentiality of the data during collection, use and transmission.

4.6.6 Audit Controls

Procedure: Each CHO will maintain and follow procedures to ensure that its project-level HMIS-compliant system maintains audit records of user activity, including attempted logins, searches conducted by each user, records altered by each user, and records added by each user. Each CHO must also establish and follow procedures to monitor these records regularly for security breaches or behavior inconsistent with the Privacy Policy outlined in **Section 6. Privacy Policy** of these policies and procedures. At minimum, this procedure must provide for monthly review of the audit records.

4.7 PII Management and Disposal

Policy: HMIS Lead and CHO users are responsible for maintaining the security of all client data extracted from the Data Warehouse or project-level HMIS-compliant system and any data collected for purposes of entry or upload to the HMIS. Users may not electronically transmit any unencrypted client data across a public network. Users must maintain the security of all hardcopy PII. CHOs are responsible for maintaining and following procedures related to data management.

4.7.1 Electronic Data Storage and Management

Procedure: All connections to the Data Warehouse for purposes of uploading data will be made over SSL connections. Any other transmission of HMIS data containing PII will be limited to secure direct connections or, if transmitted over the internet, the data will be encrypted using a 128-bit key. If PII is emailed, it must be encrypted.

The HMIS Lead and CHOs will encrypt any hard drives or removable media on which PII is stored, will download only minimal necessary data. Under no circumstances will users store PII on any personally owned media; users may not place PII on a work-owned USB drive for personal use. Data Warehouse End Users subject to NYC policies are advised that this policy does not include any use that is unlawful, violates the City's Conflicts of Interest rules or other applicable rules and regulations, or is specifically prohibited by this policy or another applicable agency policy.

Critical data and removable data devices (USB drives, CDs, external drives, etc.) must be protected by appropriate physical means from modification, theft, or unauthorized access.

Such records and confidential information contained therein remain subject to these policies and procedures. When these media have reached the end of their useful life, the data will be disposed consistent with the procedures outlined in **Section 4.7.3 Electronic and Hard Copy Disposal** of these policies and procedures.

4.7.2 Hard Copy Data Storage and Management

Hardcopies of data stored or intended to be stored in the Data Warehouse or a project-level HMIS-compliant system, regardless of whether the data has yet been uploaded to the Data Warehouse, will be treated in the following manner:

1. Records shall be kept in individual locked files or in rooms that are locked when not in use.
2. When in use, records shall be maintained in such a manner as to prevent exposure of PII to anyone other than the End User directly utilizing the record.
3. Employees shall not remove records or other information from their places of business without permission from appropriate supervisory staff unless the employee is performing a function which requires the use of such records outside of the CHO's place of business and where return of the records by the close of business of would result in the undue burden on staff.
4. When staff remove records from their places of business, the records shall be maintained in a secure location and staff must not re-disclose the PII contained in those records except as permitted by **Section 6. Privacy Policy** of these policies and procedures.
5. If records are being transmitted from one location to another, they must be placed in sealed envelopes and a receipt shall be obtained documenting the delivery of said records.
6. Faxes or other printed documents containing PII shall not be left unattended.
7. Fax machines and printers shall be kept in secure areas.
8. When faxing PII, the recipients should be called in advance to ensure the fax is properly managed upon receipt.
9. When finished faxing, copying or printing all documents containing PII should be removed from the machines promptly.

Such records and confidential information contained therein remain subject to these policies and procedures. When these materials have reached the end of their useful life, the data will be disposed consistent with the procedures outlined in **Section 4.7.3 Electronic and Hard Copy Disposal** of these policies and procedures.

4.7.3 Electronic and Hard Copy Disposal

CHOs and the HMIS Lead will establish policies and procedures for proper disposal of electronic and hard copy PII. PII shall be permanently erased when no longer needed.

CHOs and the HMIS Lead will dispose of records in accordance with the Record Retention Schedule described in **Section 6.10 Record Retention Schedule** of these policies and procedures.

4.8 Security Incidents

Policy: All HMIS End Users, both CHO and Data Warehouse, are obligated to report suspected instances of non-compliance with these policies and procedures that may leave HMIS data vulnerable to intrusion. The HMIS Lead is responsible for reporting any security incidents involving the real or potential intrusion of the Data Warehouse to the Steering Committee. Each CHO is responsible for reporting any security incidents involving the real or potential intrusion of its project-level HMIS-compliant system to the HMIS Lead.

4.8.1 Reporting Threshold

Data Warehouse users will report any incident in which unauthorized use or disclosure of PII has occurred.

CHO users will report any incident in which PII may have been used in a manner inconsistent with the CHO Privacy or Security Policies. Security breaches that have the possibility to impact the NYC HMIS must be reported to the HMIS Administrator.

Each CHO will maintain and follow procedures related to thresholds for security incident reporting.

4.8.2 Reporting Process

CHO users will report security violations to their CHO HMIS Administrator and Security Contact. The CHO HMIS Administrator will report violations to the HMIS Lead Security Officer (or designee).

FTS will regularly check the Data Warehouse for security breaches and failures and any such breaches or failures will be communicated to the HMIS Lead Security Officer and System Administrator.

The HMIS Lead Security Officer, in cooperation with the System Administrator, will review violations and recommend corrective and disciplinary actions to the Data Management Committee and the Steering Committee, as appropriate.

Each CHO will maintain and follow procedures related to internal reporting of security incidents.

5. Disaster Recovery

Policy: DSS's Emergency Preparedness and Operations Unit, housed within the Division of Security manages all major agency-wide emergencies, citywide coastal storm sheltering emergencies, and associated emergency planning activities. In the event of an emergency, in addition to performing the duties outlined by the Emergency Preparedness and Operations Unit, the HMIS Lead Project System Administrator will coordinate with FTS to ensure the Data Warehouse is functional and that data is restored according to the procedures outlined in the security plan. Each CHO must have a plan for maintaining and recovering access to its own data.

5.1 HMIS Lead

Procedure: DSS participates in NYC's Continuity of Operations Planning (COOP) program, which ensures City agencies can continue providing vital public services in the event of an emergency.

In October 2007, then Mayor Bloomberg signed a law requiring all City agencies to develop standardized COOP plans. DSS has an internal COOP team to survey its critical functions, and uses the COOP software to help them determine how to support or reinforce these functions during emergencies.

In June, 2006, then Mayor Bloomberg and the Office of Emergency Management (OEM) unveiled the City's revised Coastal Storm Plan (CSP)-the plan that is used to respond to any coastal storm that may impact the City. DSS assisted OEM with the emergency shelter planning components of the CSP, and has been tasked to lead many of the planning initiatives necessary to ensure that the Emergency Shelter system is robust and operational.

5.2 FTS

Procedure: Should access to the Data Warehouse be interrupted, FTS will contact the HMIS Lead Project System Administrator, who will communicate this message to the CHOs. The Data Warehouse is protected according to the terms of the security plan and all data will be restored to the most recent available backup day following any disaster that results in loss of data.

5.3 CHOs

Procedure: Each CHO will have a plan in place for maintaining and recovering access to its own data. Should a CHO's project-level HMIS-compliant system experience an interruption or loss of data that will have implications for the NYC HMIS, the CHO HMIS Administrator must contact the HMIS Director/Team within 5 business days.

6. Privacy Policy

6.1 Goal and Purposes

The goal of the HMIS Privacy Policy is to ensure that all required client data will be captured in the NYC HMIS while maintaining the confidentiality and security of the data in conformity with all current regulations related to the client's rights for privacy and data confidentiality.

The NYC Coalition on the Continuum of Care (CCoC) recognizes that its member agencies may have established their own privacy policies that meet the HUD privacy requirements and minimum standards set forth below. One purpose of this document is to outline those standards to all CHOs and define the parameters of compliance with these standards. The document is not intended to supplement individual CHO privacy policies. As long as CHO policies and practices meet the minimum thresholds established in this policy and do not interfere with the practices described in this policy, they may establish additional or more stringent requirements for users of their project-level HMIS-compliant system. The other purpose of this document is to describe how the HMIS Lead and the Data Warehouse meet privacy requirements established in HUD's privacy standards.

6.2 Policy Access and Amendment

Policy: The HMIS Lead may amend its privacy policy and practices at any time, subject to the approval of the CCoC. Amendments may affect data in the HMIS before the effective date of any such amendment. This policy is intended to be consistent with current privacy standards for HMIS issued by HUD.

Procedure: The Privacy Policy will be reviewed and amended consistent with the procedure described in **Section 1.5 Policy Review and Amendment** of these policies and procedures.

6.3 Applicability

Policy: The HMIS Privacy Policy applies to the HMIS Lead, the Data Warehouse, CHOs, their project-level HMIS-compliant systems, and any person accessing any HMIS data.

Procedure: The boundaries of the HMIS implementation are described in **Section 1. HMIS Overview** of these policies and procedures.

The HMIS Lead and CHOs will uphold Federal and State Confidentiality regulations to protect client records and privacy. If a CHO is covered by more stringent regulations, the more stringent regulations will prevail.

6.4 CHO Policy

Policy: Each CHO is responsible for maintaining a privacy policy and certifying that each participating project is in compliance with the NYC CCoC HMIS Privacy Policy. Each CHO's HMIS Administrator will be responsible for reviewing its privacy policy and the **Appendix C. Organization HMIS Participation Agreement** must include certification of consistency with these privacy policies. CHOs may require more rigorous privacy standards, but they must at minimum meet the privacy standards set forth in this document and must not conflict with this privacy policy. In addition, CHOs must maintain documentation about changes to their privacy policies.

Procedure: A minimal standard privacy policy is provided in **Appendix H. Example Minimal Standard CHO Privacy Policy** to these policies and procedures. Each CHO will adopt the standard policy or their own policy, so long as the policy meets the privacy standards set forth in this document and does not conflict with this privacy policy.

A CHO's Privacy Notice will:

- Specify all potential uses and disclosures of client personal information.
- Specify the purpose for collecting the information.
- Specify the time period for which the data will be retained at the organization and the method for disposing of it or removing identifiers from personal information that is not in current use 7 years after it was added to the HMIS or last changed.
- State the process and applicability of amendments, and commit to documenting all privacy notice amendments.
- Offer reasonable accommodations for persons with disabilities and/or language barriers throughout the data collection process.

- Allow the client the right to inspect and to have a copy of their client record and offer to explain any information that the individual may not understand.
- Specify a procedure for accepting and considering questions or complaints about the privacy policy.

6.5 Compliance Review

Policy: The HMIS Lead is responsible for ensuring that the HMIS implementation is operated in accordance with HUD standards. Each CHO is responsible for conducting a review annually and certifying that each participating project is in compliance with the NYC CCoC Privacy Policy and HUD standards. The CCoC, through the HMIS Lead Agency, retains the right to conduct site visits to check compliance with the privacy policy and to verify self-certification of the CHOs.

Procedure: Each CHO will indicate that they are in compliance with the HMIS Lead privacy policy on **Appendix D. Administrative and Software Certification Checklist** annually. Failure to submit this form within 30 days of its due date in any given year will be considered to be a violation of the terms of the **Appendix C. Organization HMIS Participation Agreement** and the CHO will be subject to the procedures described in **Section 3.8.3 Contract Terminations Initiated by the HMIS Lead** of these policies and procedures.

Each CHO will indicate in the **Appendix D. Administrative and Software Certification Checklist** whether or not it has either:

- Adopted the minimum standard privacy policy (provided in **Appendix H. Example Minimal Standard CHO Privacy Policy** to these policies and procedures) as their own, or
- Adopted a different privacy policy that meets the requirements outlined in the HMIS Lead privacy policy.

In the event that the CHO has adopted a more stringent privacy policy, the CHO will be expected make a copy of the policy available annually to the HMIS Lead. If no policy has been adopted at the time of execution of the **Appendix C. Organization HMIS Participation Agreement**, or at the time of the annual certifications thereafter, the CHO must establish a date not later than three months from the certification date by which such a policy will be developed and implemented. An **updated Appendix D. Administrative and Software Certification Checklist** indicating full compliance will be provided to the HMIS Lead by the target date or the CHO will be considered to be in violation of the terms of the **Appendix C. Organization HMIS Participation Agreement** and will be subject to the procedures described in **Section 3.8.3 Contract Terminations Initiated by the HMIS Lead** of these policies and procedures.

6.6 Privacy Policy Notice

Policy: The HMIS Lead and CHO must ensure that their privacy policies are readily accessible to clients and the public.

6.6.1 Public Access

Procedure: The HMIS Lead will post this NYC CCoC HMIS Policies & Procedures on the website of the CCoC (http://www.nychomeless.com) and will provide a copy to any individual upon request. CHOs that maintain websites will post their adopted privacy policy to the website.

6.6.2 Informed Client Consent

Procedure: The HMIS Lead will only use lawful and fair means to collect HMIS data. Each CHO privacy policy will include a provision stating that the CHO will only collect data with the knowledge or consent of their clients. If a client seeks their assistance, is notified that data collection will occur, and provides the CHO with HMIS data, the HMIS Lead will assume that the individual consents to the collection of information described in this policy and the CHO sharing said information with the HMIS Lead. Individual CHOs may maintain stricter policies related to getting consent from their clients to collect and share the data with the HMIS Lead.

At minimum, the HMIS Lead requires that each CHO post a sign at each intake desk or other location where data collection occurs explaining the reasons they ask for HMIS data. The sign will include the following language:

We collect personal information about homeless individuals in a computer system called a Homeless Management Information System (HMIS) for reasons that are discussed in our privacy policy. We may be required to collect some personal information by law or by organizations that give us money to operate this *program. Other personal information that we collect is important to run our programs, to improve services for homeless individuals, and to better understand the needs of homeless individuals. We only collect information that we consider to be appropriate. If you have any questions or would like to see our privacy policy, our staff will provide you with a copy.*

Agencies may use the sample attached in **Appendix H. Example Minimal Standard CHO Privacy Policy.**

6.6.3 Accessibility

Procedure: Each CHO that is a recipient of federal assistance will provide required information in languages other than English that are common in the community, if speakers of these languages are found in significant numbers and come into frequent contact with the organization.

Each CHO privacy policy must include a provision stating that they will make reasonable accommodations for persons with disabilities throughout the consent, intake, and data collection processes. This may include but is not limited to, providing qualified sign language interpreters, readers or materials in accessible formats such as Braille, audio, or large type, as needed by the individual with a disability.

6.7 HMIS Data Use and Disclosure

Policy: The confidentiality of the data collected in the HMIS must be protected. CHOs must collect data by legal and fair means, consistent with **Section 6.6.2 Informed Client Consent** of these policies and procedures. The HMIS Lead and CHOs may only collect, use, and disclose these data for the specific purposes and reasons defined in this section.

The HMIS Lead collects HMIS data from homeless service organizations that upload data into a Data Warehouse. These data are collected only for specific purposes of carrying out the duties of the CHO, the HMIS Lead, or when required by law. HMIS data may only be collected, used, or disclosed for activities described in this section. The HMIS Lead or CHOs may or may not make any of these uses or disclosures of HMIS data. The HMIS Lead requires that individuals that seek assistance from a CHO are notified that data collection, use, and disclosure will occur. By uploading data to the Data Warehouse, the CHO verifies that individuals have provided the CHO with consent to the use or disclosure of their HMIS data for the purposes described below and for other uses and disclosures that the HMIS Lead determines to be compatible with these uses or disclosures:

- To provide or coordinate individual case management services;
- For functions related to payment or reimbursement for services;
- To carry out administrative functions, including but not limited to audit, personnel oversight, and management functions;
- To produce aggregate-level reports regarding use of services;
- To create de-identified (anonymous) information;
- To track project-level outcomes;
- To identify unfilled service needs and plan for the provision of new services;
- To conduct a study or research project approved by DSS Office of Evaluation and Research (OER);
- When required by law to the extent that use or disclosure complies with and is limited to the requirements of the law;
- To avert a serious threat to health or safety if:
  - The use or disclosure is reasonably believed to be necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and
  - The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.
- To report about an individual reasonably believed to be a victim of abuse, neglect or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence in any of the following three circumstances:
  - Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;
  - If the individual agrees to the disclosure; or
  - To the extent that the disclosure is expressly authorized by statute or regulation and either of the following are applicable:

- The CHO believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
- If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the HMIS data for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure;

When such a permitted disclosure about a victim of abuse neglect or domestic violence is made, the individual making the disclosure will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:

- In the exercise of professional judgment, it is believed that informing the individual would place the individual at risk of serious harm; or
- It would be informing a personal representative (such as a family member or friend), and it is reasonably believed that the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as we determine in the exercise of professional judgment.

- To a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
  - In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;
  - If the law enforcement official makes a written request for HMIS data that:
    - Is signed by a supervisory official of the law enforcement agency seeking the HMIS data;
    - States that the information is relevant and material to a legitimate law enforcement investigation;
    - Identifies the HMIS data sought;
    - Is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
    - States that de-identified information could not be used to accomplish the purpose of the disclosure.
  - If it is believed in good faith that the HMIS data constitutes evidence of criminal conduct that occurred on the CHO's premises;
  - In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the HMIS data disclosed consists only of name, address, date of birth, place of birth, social security number and distinguishing physical characteristics; or
  - If:
    - The official is an authorized federal official seeking HMIS data for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others); and
    - The information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.
- To comply with government reporting obligations for HMIS and for oversight of compliance with HMIS requirements.
- To third parties for the following purposes:
  - To permit other systems of care to conduct data matches (i.e., to determine if you are also utilizing services from such other systems of care); and
  - To permit third party research firms and/or evaluators to perform research and evaluation services, approved by DSS Office of Evaluation and Research (OER), in connection with the projects administered by the HMIS Lead and the CHOs;

  Provided that before client-level HMIS data are disclosed under this subsection, the third party that will receive such client-level HMIS data and use it as permitted above must first execute a Data Use & Disclosure Agreement requiring such third party to comply with all applicable laws and regulations, including the privacy standards and disclosure provisions contained in the current Department of Housing and Urban Development Homeless Management Information Systems Data and Technical Standards, which such standards and provisions are reflected herein.

The HMIS Lead may share client level HMIS data with contracted entities as follows:

- The CHO originally uploading the data to the NYC HMIS;
- Outside organizations under contract with the HMIS Lead or other entity acting on behalf of the CCoC for research, data matching, and evaluation purposes. The results of this analysis will always be reported in aggregate form; client level data will not be publicly shared under any circumstance.

Any requests for reports or information from an individual or group who has not been explicitly granted access to the NYC HMIS will be directed to the CCoC Steering Committee. No individual client data will be provided to meet these requests without proper authorization.

Before any use or disclosure of PII that is not described here is made, the HMIS Lead or CHO wishing to make the disclosure will seek the consent of any individuals whose PII may be used or disclosed.

6.8 Access and Correction

Policy: Clients whose data is collected in HMIS may inspect and have a copy of their HMIS record by requesting it from the CHO that originally collected the information. The HMIS Lead requires that the CHO establish a policy to manage such requests and to explain any information that a client may not understand.

Procedure: Each CHO will describe in its privacy policy how it will manage requests from clients for correction of inaccurate or incomplete HMIS records. This policy will allow for a client to request to see their HMIS data or request that data be removed from the HMIS. Nothing in this section is intended to indicate that a CHO is released from any obligation by any funder to collect required data elements.

If the CHO agrees that the information is inaccurate or incomplete, they may delete it or they may choose to mark it as inaccurate or incomplete and to supplement it with additional information. Any such corrections applicable to the data stored in the Data Warehouse will be made at the time of the next upload.

A record of these transactions will be kept by the CHO HMIS Administrator. In response to requests to view his/her data in the HMIS, the CHO HMIS Administrator or case manager will provide a copy of the requested data within a reasonable time frame to the client.

CHOs are permitted to establish reasons for denying client requests for inspection of HMIS records. These reasons are limited to the following:

- If the information was compiled in reasonable anticipation of litigation or comparable proceedings;
- If the record contains information is about another client or individual (other than a health care provider or homeless provider) and the denial is limited to the section of the record containing such information;
- If the information was obtained under a promise of confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information; or
- Disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

If a CHO denies a request for access or correction, the CHO will explain the reason for the denial. The CHO will also maintain documentation of the request and the reason for the denial.

CHOs may reject repeated or harassing requests for access to or correction of an HMIS record.

6.9 Data Retrieval and Sharing

Policy: As the HMIS Lead Agency, the DSS Federal Reporting and Homelessness Policy unit and associated staff, have access to retrieve all data in the NYC HMIS. Other DSS staff members may have limited access to client level HMIS data for the purposes of supporting the Federal Reporting and Homelessness Policy unit.

CHOs may share PII with each other, provided they have executed a data sharing agreement outlining roles, responsibilities, parameters of data sharing, and the steps that will be taken if one party withdraws from the data sharing agreements.

Procedure: HMIS as implemented in NYC is a system which can provide reports required by HUD, the Continuum of Care, and other stakeholders at a reporting level that does not identify individuals but can provide accurate statistical data including, numbers served, trend assessments, and non-duplicated statistical reports based on data entered into the NYC HMIS by CHOs. Data from the NYC HMIS will be used to produce these CCoC and local level statistical reports required by HUD and will be used in various HUD applications and reports. These uses are included in the uses and disclosures described in **Section 6.7 HMIS Data Use and Disclosure** of these policies and procedures.

Data sharing between CHOs for the purpose of coordinating services is also included in the allowable uses and disclosures described in **Section 6.7 HMIS Data Use and Disclosure** of these policies and procedures.

6.10 Record Retention Schedule

Policy: The HMIS Lead may keep information for a period of more than 7 years (the minimum required by the HMIS Security and Privacy Regulations) if required to do so by an applicable statute, regulation, contract or other requirement.

Similarly, CHOs are required to establish a policy to dispose of or de-identify PII not in current use seven years after the information was created or last changed unless prohibited from doing so by an applicable statute, regulation, contract or other requirement.

Procedures: The HMIS Lead will coordinate with FTS to ensure that data in the Data Warehouse is retained according to the policies and procedures. CHOs will include a provision in their policies and procedures to comply with this policy.

6.11 Grievance

Policy: Concerns related to the HMIS Privacy Policy may be raised according to the procedures outlined in **Section 2.6 Client Grievance Against HMIS Lead** of these policies and procedures. CHOs must establish a policy and regular process for receiving and reviewing complaints from clients about potential violations of the policy.

Procedure: CHOs should report any violation of their privacy policy to the HMIS Lead. In addition to any actions taken by the CHO to sanction the employee, depending on the frequency, prior training, severity, intent, etc., of the violation, the HMIS Lead may report the findings to the Steering Committee or law enforcement, as appropriate, for further action. Such action may include,

- Suspension of system privileges; or
- Revocation of system privileges.

Sanctions can be appealed to a group comprised of the Steering Committee and any necessary ad hoc members.

7. Data Quality Plan

7.1 Goal

Data from the NYC HMIS will be used to document Continuum of Care needs, performance, and to document services provided to the homeless. The NYC HMIS will provide statistics and outcome measures for reports to HUD, the Steering Committee, and other stakeholders.

For NYC HMIS to be able to provide accurate and timely information, HMIS participation must be maximized, data must be collected by CHOs regularly, completely, and accurately, and data must be uploaded to the NYC HMIS in a timely manner. This will permit the HMIS Lead to produce reports related to the annual evaluation, the HUD System Performance Measures, Emergency Solutions Grants-Consolidated Annual Performance and Evaluation Report (ESG-CAPER), the Housing Inventory Count (HIC), the Point in Time Count (PIT), and the Longitudinal System Analysis (LSA) (formerly known as the Annual Homeless Assessment Report (AHAR)). In addition, improved participation and data quality will enhance the competitiveness of the CCoC in the annual HUD competition.

The goal of these HMIS Data Quality policies and procedures is to standardize expectations and provide guidance to HMIS participating projects on the extent and quality of data entered into the NYC HMIS so as to be able to draw reasonable conclusions about the extent of homelessness and the impact of homeless services.

7.2 HMIS Participation Thresholds

Policy: 100% of all programs funded by Emergency Solutions Grant-ESG, CoC, Veterans Grant Per Diem (GPD), VA Community Contract, HUD-VASH, Supported Services for Veterans and their families (SSVF), Contract Residential Services VA-CRS , Community Contracts Safe Haven Programs VA-HCHV/SH, VA-Compensated Work Therapy – Transitional Residence (CWT/TR) and Prevention Assistance and Temporary Housing (PATH) projects are required to participate in HMIS, as stated in **Section 1. HMIS Overview** of these policies and procedures.

In addition, the CCoC aspires to have 100% of all projects primarily dedicated to serving homeless persons in NYC participate in HMIS.

Procedure: The HMIS Lead will maintain a listing of all continuum lodging and services projects' participation in HMIS. On a quarterly basis, the status of each project will be updated and reported to the Data Management Committee (DMC). Each project will be indicated as "fully participating," "uploading incomplete data," "implementing," or "not yet participating."

7.3 Minimum Required Data Elements

Policy: Each CHO is required to collect and submit all required program descriptor data elements to the HMIS Lead prior to initial setup in the HMIS, at the time of any change to any project descriptor data element (e.g. number of beds/units operated or type of households served) and annually thereafter. In addition, each CHO is required to upload records on all clients participating in each HMIS participating project. A record comprises, at minimum, all Project Descriptor, Universal Data Elements, Program-Specific Data Elements, and Metadata Elements applicable to the project type and meets the accuracy, completeness, and timeliness standards outlined in these policies and procedures. The required data elements, along with detailed definitions and explanations are provided in NYC HMIS Data Dictionary, included as **Appendix I. NYC HMIS Data Dictionary** to these policies and procedures.

Procedure: Each CHO will begin collecting the data as per the 2017 HMIS Data Standards by October 1, 2017. This means all required Project Descriptor, Universal, Program Specific, and Metadata elements for the appropriate subjects (head of household, head of household and other adults, all clients) at the specified data collection points (record creation, project entry, annual assessment, update, and project entry).

Each CHO will provide all required project descriptor data elements for each participating project via the Project Information Form incorporated into the **Appendix C. Organization HMIS Participation Agreement** as described in **Section 3. CHO HMIS Participation Policies** of these policies and procedures. The **Project Information Form** is provided in **Appendix F**.

Each CHO will upload complete records on all clients in each HMIS participating project to the Data Warehouse at least once per month, no later than the tenth business day. The HMIS Lead will maintain the NYC Data Standards consistent with HUD's most current HMIS Data Standards. The HMIS Director/Team will be responsible for communicating any updates to the NYC Data Standards to each CHO HMIS Administrator and for providing trainings to them to ensure that they, in turn, are able to train their End Users on the changes. The full HUD Data Standards can be found on HUD's OneCPD Resource Exchange at https://www.onecpd.info/hmis/.

7.4 Data Collection and Upload Standards

Policy: The HMIS Lead is responsible for the overall HMIS data quality. In an effort to maintain that quality, the HMIS Lead has established data quality thresholds for participating projects to meet the terms of their **Appendix C. Organization HMIS Participation Agreements**. Each CHO is responsible for developing and implementing policies to ensure that its End Users are entering data into the project-level HMIS-compliant system in a timely, complete, and accurate manner. The HMIS Lead and CHOs are jointly responsible for ensuring that project data in the HMIS meets the thresholds outlined in this section. In order to develop consistency in data collection processes and develop capacity among End Users, the Data Management Committee and the HMIS Lead may establish an HMIS user group.

7.4.1 Timeliness

The purpose of timeliness is to ensure access to data when it is needed – either proactively (for planning or monitoring purposes, or to meet reporting requirements) or reactively (in response to a request for information or to respond to inaccurate information).

Standards:

All HMIS participating projects will ensure entry of data for new clients, services provided to new and existing clients, and exits for each month are uploaded to the NYC Data Warehouse by the 10th business day of the following month. Any corrections that may need to be made to address technical or data quality issues must be resolved no later than the 10th business day of the following month.

The 2017 Data Standards have six data collection points: record creation, project start, at occurrence, at update, annual assessment (done within 30 days before or 30 days after project admission date), and project exit. Each CHO will develop and implement a policy requiring that all client data be entered into the project-level HMIS-compliant system in accordance with the requirements of the data collection points. Data collected for update should be entered within three business days.

Each CHO will indicate in the Administrative and Software Certification whether or not such a policy exists. If such a policy does not exist at the time of execution of the **Appendix C. Organization HMIS Participation Agreement**, or at the time of the annual certifications thereafter, the CHO must establish a date not later than three months from the certification date by which such a policy will be developed and implemented. A copy of the policy must be made available to the HMIS Lead by the target date or the CHO will be considered to be in violation of the terms of the **Appendix C. Organization HMIS Participation Agreement.**

7.4.2 Completeness

The purpose of completeness is to ensure sufficient data on clients, their demographic characteristics, and service use to facilitate confident reporting and analysis on the extent and characteristics of the homelessness including:

- Unduplicated counts of clients served in the continuum of care;
- Patterns of use of people entering and exiting the homeless assistance system; and
- Evaluation of the effectiveness of homeless systems.

Standards:

The goal is that ALL projects participating in the NYC HMIS will have complete data; however, residential projects with less than 90% data completeness and Street Outreach projects with less than 75% data completeness will be considered to be in violation of their **Appendix C. Organization HMIS Participation Agreement** and will be subject to the process described in **Section 3.8.3 Contract Terminations Initiated by the HMIS Lead** of these policies and procedures.

This will be evaluated by the HMIS Lead on a semi-annual basis and will be calculated as an overall percentage of all required data fields for all clients active during the quarter. The HMIS Lead will provide an annual report at minimum to the CHOs. detailing the number of clients added in the quarter, active in the quarter, and the missing/ don't know/ refused/ data not collected rate for each data element for clients active during the quarter. This report will be the basis of determining if the project is meeting the standards and is intended to assist the CHO in identifying and correcting missing data in its project-level HMIS-compliant system and discrepancies between the project-level HMIS-compliant system and the Data Warehouse (if any). In addition, the HMIS Lead will provide guidance to CHO'S on specific data elements and on specific goals and objectives in system wide performance areas as identified by the CoC Steering Committee.

<u>The expectation is that there is no missing data</u>. In the event data was not collected, however, the "client doesn't know," "missing information," and "client refused" responses should not be used. These response options are expected to indicate that the client did not know a response or that the client refused to respond, not that the case manager or other user did not know the response or refused to collect the information. All Universal and Program Specific Data elements are required, and so it is expected that it is very unlikely that any field would be left blank.

7.4.3 Accuracy

The purpose of accuracy is to ensure that the data housed in the CCoC HMIS is the best possible representation of reality as it relates to homeless people and the projects that serve them. Accuracy is determined by assessing the truthfulness by the client, the accuracy of the data collected by staff, and the accuracy of the data entered into the system by the staff. CHOs are responsible for making these assessments. In the Data Warehouse, accuracy is assessed by verifying consistency across all forms of reporting: Notice of Funding Availability (NOFA) Project Applications, Annual Performance Report (APR), CCoC Evaluation and any other similar reports.

Standard:

The goal is to make sure HMIS data is entered correctly and can be verified with documentation. CHOs are expected to regularly check the accuracy of the information provided against other reliable sources and perform checks on data elements such as date of birth (e.g. no negative ages or dates after the present entered for this field), veteran status (children are not categorized as veterans), disability status (someone who receives Social Security Income is not categorized as having no disabilities) "Client Refused," "Missing Information," or "Client Does Not Know," will also not continue to be accepted for categories such as race, ethnicity, prior living arrangement, and length of stay in prior living arrangement. Data indicating unaccompanied children will be immediately identified and verified as accurate or corrected.

Each CHO will develop and implement an internal business process for conducting logic checks (such as those suggested in the paragraph above) on the data in its project-level HMIS-compliant system and regularly comparing universal and program specific data elements to available paper records and updating/correcting missing or inaccurate data. Each CHO will develop and implement an internal process that engages both intake and data entry staff to ensure collaboration and communication focused on input of accurate client data into the HMIS system.

Each CHO will indicate in the Administrative and Software Certification whether or not such a policy exists. If such a policy does not exist at the time of execution of the **Appendix C. Organization HMIS Participation Agreement**, or at the time of the annual certifications thereafter, the CHO must establish a date not later than three months from the certification date by which such a policy will be developed and implemented. A copy of the policy must be made available to the HMIS Lead by the target date or the CHO will be considered to be in violation of the terms of the **Appendix C. Organization HMIS Participation Agreement.**

The HMIS DSS Team will be authorized to conduct occasional checks to verify reports generated from the Data Warehouse are consistent with a CHO's NOFA Project Applications, APR, CCoC Evaluation, client case file data, and any other similar reports. Projects will be required to address any discrepancies that are observed, and projects found to have many such discrepancies will be required to meet with the DSS HMIS Team, referred to the Performance and Quality Improvement Committee (PQI) process, Data Management Committee (DMC) and/or the Steering Committee Co-Chairs.

7.5 Data Quality Monitoring

Policy: The HMIS Lead is responsible for monitoring CHOs to ensure that the standards on the extent and quality of data entered into the NYC HMIS that have been set forth in these policies and procedures are met to the greatest possible extent and that data quality issues are quickly identified and resolved. Each CHO is responsible for addressing any issues identified through the process of this monitoring prior to the next scheduled upload to the Data Warehouse. Any CHO failing to meet the data quality standards as averaged over the calendar year will be considered to be in violation of the terms of the **Appendix C. Organization HMIS Participation Agreement** and will be subject to the procedures described in **Section 3.8.3 Contract Terminations Initiated by the HMIS Lead** of these policies and procedures.

7.5.1 Data Quality Monitoring

The HMIS Lead will be following-up with Providers and FTS quarterly and monthly in some instances to ensure that data is meeting performance standards. Results will be shared with the Providers and FTS, and monitored by the CoC Data Management Committee, and CoC Steering Committee, and shared with the Provider community at-large if necessary. Providers can expect to be contacted more frequently by the HMIS Lead to request explanations around some data entry elements, which may lead to requests for data clean-up and re-submission, and to schedule corrective action plans if needed. FTS can also expect frequent communication with the HMIS Lead to review data reports, discuss random sampling of data to test for quality, and to review how FTS is maintaining data standards and quality in AWARDS.

7.5.2 Data Quality Reporting

Procedure: The HMIS Lead will run project-level data completeness, length of stay, and bed utilization rate reports as described in the preceding section on a semi-annual basis and will directly provide agencies with the reports for their projects via email. The monitoring will be shared in the following ways:

- Data Management Committee Review: The CCoC Data Management Committee will review a semi-annual CHO report results. The CCoC Data Management Committee will work with HMIS participating agencies to identify training needs to improve data quality.
- CoC Review: The CCoC Data Management Committee will share HMIS participation rates and project-level data completeness status with the CCoC Steering Committee semi-annually.
- Public Review: HMIS participation rates and project-level data completeness rates will be posted to the CCoC website on a quarterly basis.

7.5.3 Remediation

Procedure: Any project failing to meet the data completeness thresholds for any given quarter will make appropriate corrections in time for the subsequent month's data upload (in other words, the project will have between 30 to make corrections). CHOs with repeated data quality issues may be provided additional training, referred to the PQI process, or considered to be in breach of their **Appendix C. Organization HMIS Participation Agreement**. The Data Management Committee will review reports and provide recommendations for additional measures.

NYC CCOC Coalition on the Continuum Of Care

Appendix A: Data Warehouse User Guide

This appendix is provided as a reference for HMIS-contributing organizations. It consists of four sections:
Section 1: Completing data uploads from within AWARDS to the NYC HMIS
Section 2: Completing data uploads from Non-AWARDS databases to NYC HMIS
Section 3: Accessing the Help Desk
Section 4: Cheat Sheet for Non-Awards Users

The NYC HMIS Data Warehouse can be accessed here: https://nychmis.footholdtechnology.com/

Section 1:
Completing data uploads from within AWARDS to the NYC HMIS

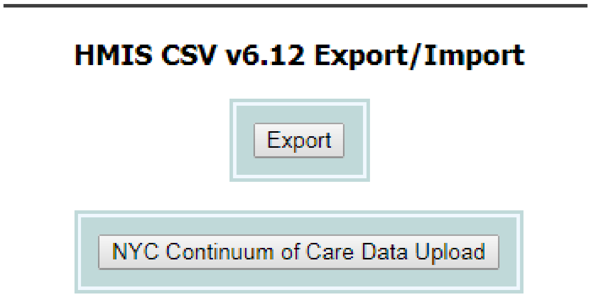
FOR AWARDS USERS

Please Note: Additional support can be accessed via the AWARDS Help Desk for the steps described below. See Item 2 for more information.

Authorized users see a button on the System Set up module's menu page labeled "HMIS Data Export." Once an agency designates an authorized user, the Foothold Client Services Representative can add this user to the list of authorized uploaders in AWARDS. **Users should not begin uploading to NYC's HMIS Data Warehouse until you receive confirmation from your Foothold Client Services Representative your database is ready to contribute data.**

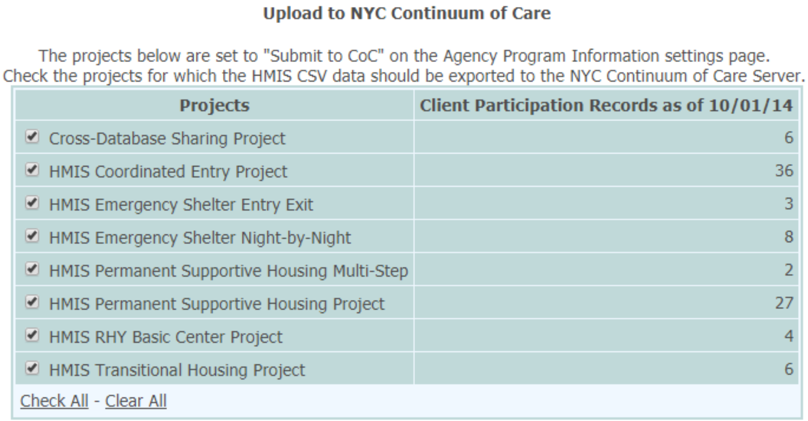
To upload data to the NYC HMIS Data Warehouse complete the following steps:

1. From the *AWARDS Opening Menu* page, click **Administration**. The *Administration* page is displayed.
2. Click **System Setup**. The *System Setup* fly-out is displayed.
3. Click **HMIS Data Export**. The *HMIS Data Export* page is displayed.


HMIS CSV v6.12 Export/Import
Export
NYC Continuum of Care Data Upload

2. Click the **NYC Continuum of Care Data Upload** button. The *Export to NYC HMIS* page is displayed.

3. The *Export to NYC HMIS* page displays a table showing the programs set to submit to the NYC HMIS, along with the number of program participation records to be exported for each program. If the information displayed is correct, click **Validate Records**. The *Validation in Progress* page is displayed.



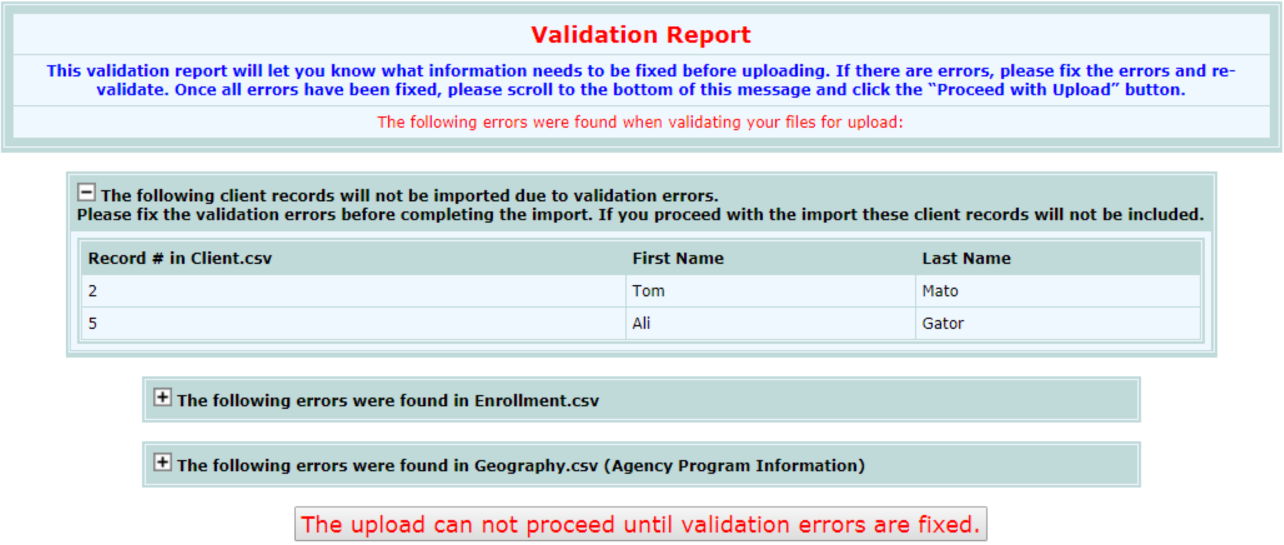
Upload to NYC Continuum of Care

The projects below are set to "Submit to CoC" on the Agency Program Information settings page.
Check the projects for which the HMIS CSV data should be exported to the NYC Continuum of Care Server.

Projects	Client Participation Records as of 10/01/14
☑ Cross-Database Sharing Project	6
☑ HMIS Coordinated Entry Project	36
☑ HMIS Emergency Shelter Entry Exit	3
☑ HMIS Emergency Shelter Night-by-Night	8
☑ HMIS Permanent Supportive Housing Multi-Step	2
☑ HMIS Permanent Supportive Housing Project	27
☑ HMIS RHY Basic Center Project	4
☑ HMIS Transitional Housing Project	6

Check All - Clear All

4. On the *Validation in Progress* page click **Messages.** The *messages* module will be displayed.
5. You will receive a separate *Validation Report* message for each project you selected to upload to NYC HMIS. Click on the first message. The report will contain the HUD CSV errors for the project. You cannot complete an upload until all client level errors are fixed. If you have client level errors your report will contain the following:



Validation Report

This validation report will let you know what information needs to be fixed before uploading. If there are errors, please fix the errors and re-validate. Once all errors have been fixed, please scroll to the bottom of this message and click the "Proceed with Upload" button.

The following errors were found when validating your files for upload:

⊟ **The following client records will not be imported due to validation errors.**
Please fix the validation errors before completing the import. If you proceed with the import these client records will not be included.

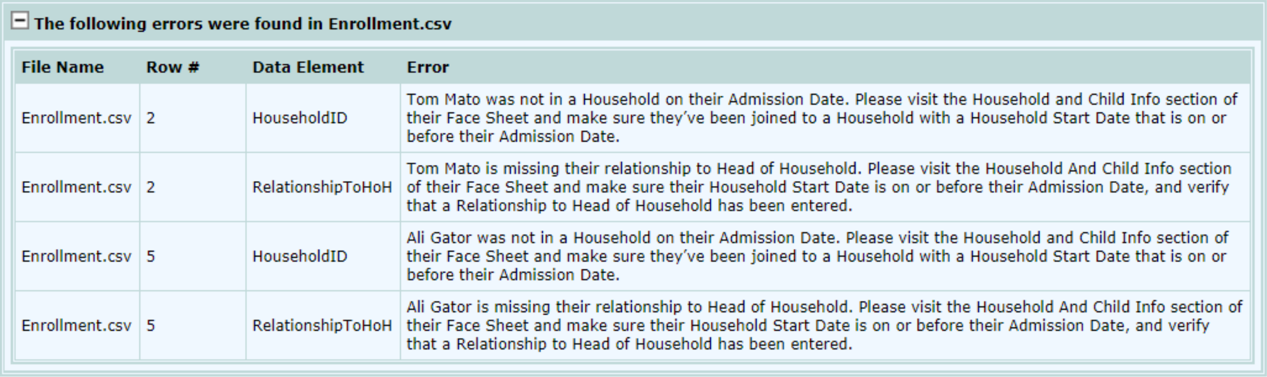
Record # in Client.csv	First Name	Last Name
2	Tom	Mato
5	Ali	Gator

⊞ **The following errors were found in Enrollment.csv**

⊞ **The following errors were found in Geography.csv (Agency Program Information)**

The upload can not proceed until validation errors are fixed.

6. Click the plus button next to the CSV file which contains the client level errors. The errors will be displayed. Pay particular attention to Enrollment.csv, Exit.csv, and Disabilities.csv. In this example, the errors are in *Enrollment.csv*.

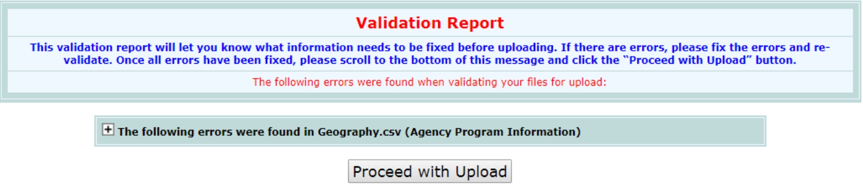


⊟ The following errors were found in Enrollment.csv

File Name	Row #	Data Element	Error
Enrollment.csv	2	HouseholdID	Tom Mato was not in a Household on their Admission Date. Please visit the Household and Child Info section of their Face Sheet and make sure they've been joined to a Household with a Household Start Date that is on or before their Admission Date.
Enrollment.csv	2	RelationshipToHoH	Tom Mato is missing their relationship to Head of Household. Please visit the Household And Child Info section of their Face Sheet and make sure their Household Start Date is on or before their Admission Date, and verify that a Relationship to Head of Household has been entered.
Enrollment.csv	5	HouseholdID	Ali Gator was not in a Household on their Admission Date. Please visit the Household and Child Info section of their Face Sheet and make sure they've been joined to a Household with a Household Start Date that is on or before their Admission Date.
Enrollment.csv	5	RelationshipToHoH	Ali Gator is missing their relationship to Head of Household. Please visit the Household And Child Info section of their Face Sheet and make sure their Household Start Date is on or before their Admission Date, and verify that a Relationship to Head of Household has been entered.

7. Follow the directions within the **Error** column to fix the error. Errors are fixed within the client's project record in AWARDS. In this example, you would navigate to the client's face sheet – household composition and verify their household start date is on or before their project admission date. For more information on how to fix CSV validation errors, please view the following film:
   https://demodb.footholdtechnology.com/training/films/HMISValid.html
   Additional troubleshooting information is also available in AWARDS online help:
   https://demodb.footholdtechnology.com/help/?11874
8. Follow steps 5-7 for each project you are uploading to NYC HMIS. This will help you fix all your client level errors for all uploading projects

9. Once you have fixed the applicable client errors **for all uploading projects**, return to step 1 and complete the sequential steps. If you have successfully fixed your client level errors, you will see a **Proceed with Upload** button within your *Validation Report*. When you are ready, click **Proceed with Upload**.



Validation Report

This validation report will let you know what information needs to be fixed before uploading. If there are errors, please fix the errors and re-validate. Once all errors have been fixed, please scroll to the bottom of this message and click the "Proceed with Upload" button.

The following errors were found when validating your files for upload:

⊞ The following errors were found in Geography.csv (Agency Program Information)

The *Export Running* page notes an export report will be sent via the AWARDS Messages module once the export is complete. Click the **messages** link on this page. You will receive two messages about the status of your export. The first will say your export "has been added to queue." **NOTE: this message does not mean that the upload has been successfully completed!** Once the export is complete, a message labeled "Upload Complete" will appear in the Inbox. This message will contain information regarding the status of the completed upload.

The process of uploading data to the NYC HMIS Data Warehouse is now complete.

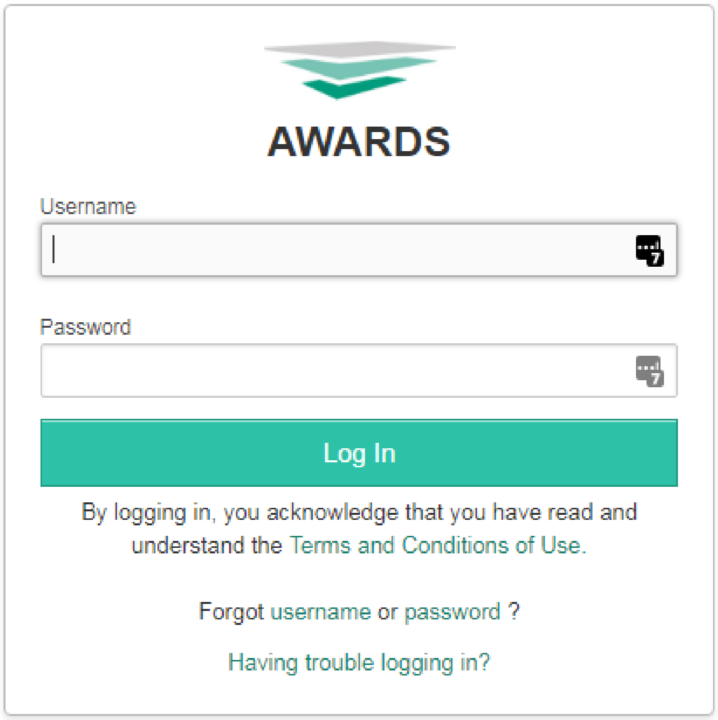
Section 2:
Completing data uploads from Non-Awards databases to the NYC HMIS

FOR NON-AWARDS USERS

Please Note: Additional support can be accessed via the AWARDS Help Desk for the steps described below. See Item 2 for more information.

The first step in the upload process is to gain access to the NYC HMIS Data Warehouse. DSS will provide you with a unique Login ID and Password for a designated staff member at your agency. Once this information has been received, the following steps can be followed:

1. Open any Internet Browser window and type https://nychmis.footholdtechnology.com into the address bar. This will open the AWARDS Login Screen.

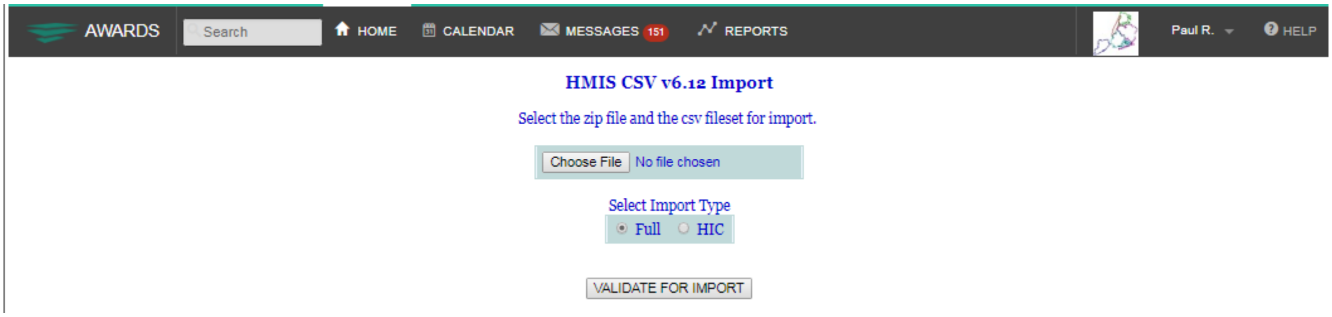


By logging in, you acknowledge that you have read and understand the Terms and Conditions of Use.

2. Type your **Login ID** (provided by NYC COC) into the Login ID field
3. Type your **Password** (provided by NYC COC) into the Password field.
4. Click the **LOGIN to AWARDS** button. The database will then open to the AWARDS Opening Menu.
5. From the *AWARDS Opening Menu* page, click **Administration**. The *Administration* page is displayed.
6. Click **System Setup**. The *System Setup* fly-out is displayed.
7. Click **HMIS Data Export**. The *HMIS Data Export* page is displayed.
8. Click **Import**. The *HMIS CSV Import* page is displayed.

*Please note: Some older logins will display a limited HMIS Menu page when a user logs in. For these users, click **Upload Data**.*

The *HUD HMIS CSV format* page is displayed. For each of the seventeen files making up the CSV upload, users will see a “Choose File” button that will allow them to locate **and select the corresponding file on the user’s local machine.**



HMIS CSV v6.12 Import

Select the zip file and the csv fileset for import.

Choose File No file chosen

Select Import Type
● Full ○ HIC

VALIDATE FOR IMPORT

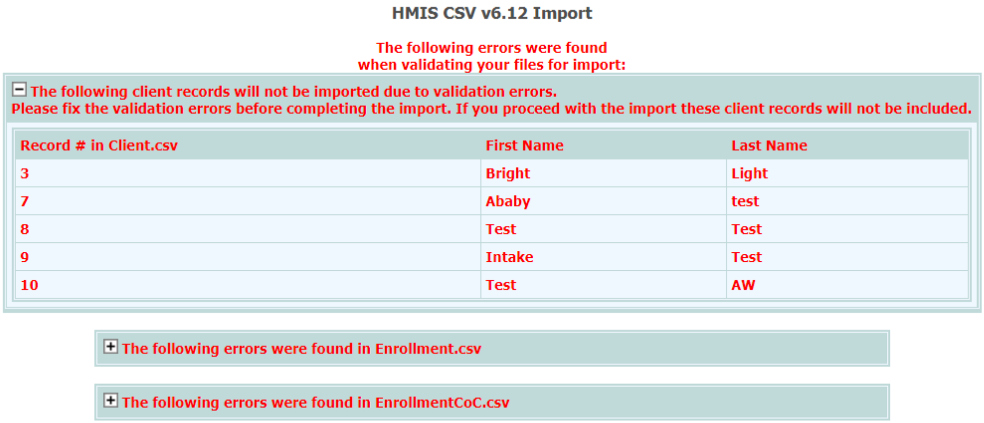
After clicking **Choose File,** select the pre-assembled .zip file with, at a minimum, the following CSV files:

Affiliation.csv Client.csv Disabilities.csv Enrollment.csv EmploymentEducation.csv
EnrollmentCoC.csv Exit.csv Export.csv Funder.csv Geography.csv
HealthAndDV.csv Inventory.csv Services.csv Organization.csv IncomeBenefits.csv
Project.csv ProjectCoC.csv

Please note: The file names can be altered from the listed names so long as the Export.csv file lists all of the correctly named files as contained in the .zip file. The .zip file can be named anything but must have the ".zip" extension.

File Value Guidance: Please refer to the HMIS CSV Format Specifications v6.12 found here: https://hudhdx.info/Resources/Vendors/5_1_2/HMISCSVSpecifications6_12.docx

8. Once the user browses their local machine and identifies the .zip file for import, clicking **VALIDATE FOR IMPORT** uploads the file and evaluates the individual CSV files for format and content. If there are errors found in the file, the user is notified of the errors. Each file containing an error is highlighted with an expandable list of error details. **Uploaders should fix all errors which exclude a client.** These clients will be listed at the top of the validation results.



HMIS CSV v6.12 Import

The following errors were found
when validating your files for import:

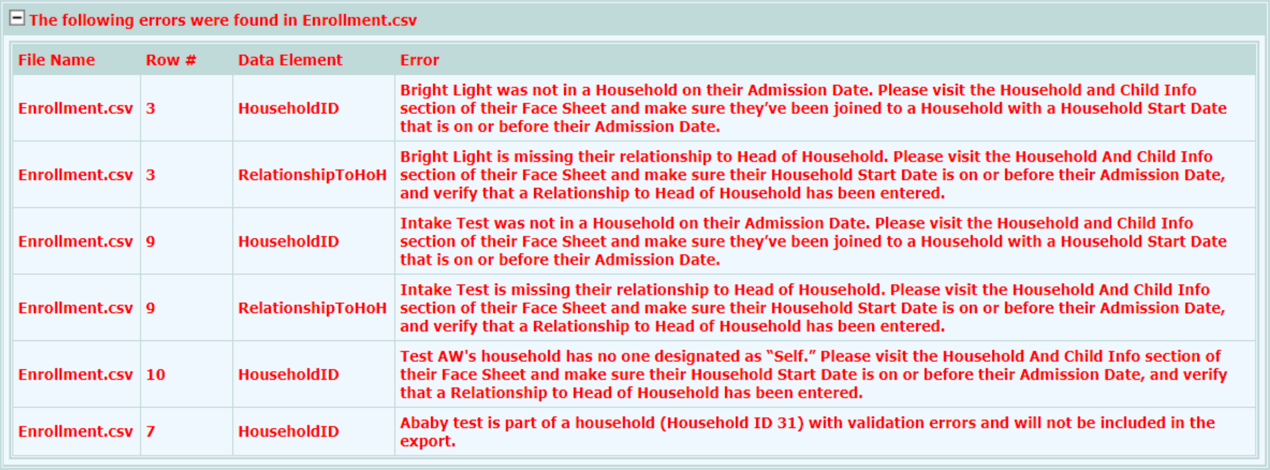
⊟ The following client records will not be imported due to validation errors.
Please fix the validation errors before completing the import. If you proceed with the import these client records will not be included.

Record # in Client.csv	First Name	Last Name
3	Bright	Light
7	Ababy	test
8	Test	Test
9	Intake	Test
10	Test	AW

⊞ The following errors were found in Enrollment.csv

⊞ The following errors were found in EnrollmentCoC.csv

9. Click the plus button next to the CSV file which contains the client level errors. The errors will be displayed. Pay particular attention to Enrollment.csv, Exit.csv, and Disabilities.csv In this example, the errors are in *Enrollment.csv*.



⊟ The following errors were found in Enrollment.csv

File Name	Row #	Data Element	Error
Enrollment.csv	3	HouseholdID	Bright Light was not in a Household on their Admission Date. Please visit the Household and Child Info section of their Face Sheet and make sure they've been joined to a Household with a Household Start Date that is on or before their Admission Date.
Enrollment.csv	3	RelationshipToHoH	Bright Light is missing their relationship to Head of Household. Please visit the Household And Child Info section of their Face Sheet and make sure their Household Start Date is on or before their Admission Date, and verify that a Relationship to Head of Household has been entered.
Enrollment.csv	9	HouseholdID	Intake Test was not in a Household on their Admission Date. Please visit the Household and Child Info section of their Face Sheet and make sure they've been joined to a Household with a Household Start Date that is on or before their Admission Date.
Enrollment.csv	9	RelationshipToHoH	Intake Test is missing their relationship to Head of Household. Please visit the Household And Child Info section of their Face Sheet and make sure their Household Start Date is on or before their Admission Date, and verify that a Relationship to Head of Household has been entered.
Enrollment.csv	10	HouseholdID	Test AW's household has no one designated as "Self." Please visit the Household And Child Info section of their Face Sheet and make sure their Household Start Date is on or before their Admission Date, and verify that a Relationship to Head of Household has been entered.
Enrollment.csv	7	HouseholdID	Ababy test is part of a household (Household ID 31) with validation errors and will not be included in the export.

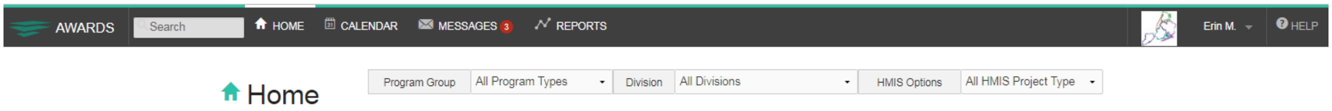
10. Errors which exclude a client should be fixed in user's home system or within the CSV file itself, to the best of the uploading agency's ability. Specific steps to fix errors will be unique to the platform the uploader is using. If the errors are critical, the import is suspended and the user is directed to correct the errors. Examples of critical errors include: missing files, incorrectly formatted files, or unknown programs.
11. Once critical and errors which exclude a client are fixed, return to step 5 and validate your files for upload. Click **IMPORT.**
12. Clicking **IMPORT** completes the importing process The Import in Progress page notes an import report will be sent via the AWARDS Messages module once the import is complete. Click the messages link on this page. You will receive two messages about the status of your import. The first will say your import "has been added to queue." **NOTE: this message does not mean that the import has been successfully completed!** Once the import is complete, a message labeled "Import #xxxx Results" will appear in the Inbox. This message will contain information regarding the status of the completed import.

The process of uploading data to the NYC HMIS Data Warehouse is now complete.

Section 3:
Accessing the Help Desk

Before you contact the Help Desk, it is strongly recommended you complete a thorough review of AWARDS online help resources.

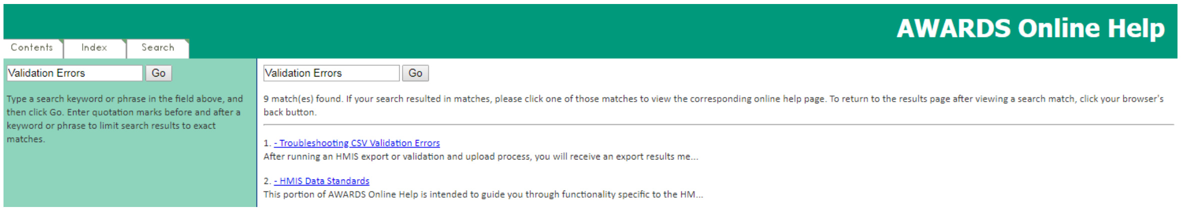
1. You can access AWARDS online help via the **Help** menu in the top right corner of your screen. In the selection list, select **AWARDS Online Help.**



Program Group: All Program Types
Division: All Divisions
HMIS Options: All HMIS Project Type

In many cases you will be able to find the information you are looking for very quickly, and as a result will not need to contact the Help Desk, which can be a lengthier process.

2. Click the **Search** tab on the right side of the page. To complete a search, enter a keyword or phrase in the available field and click **Go**.



Validation Errors

Type a search keyword or phrase in the field above, and then click Go. Enter quotation marks before and after a keyword or phrase to limit search results to exact matches.

Validation Errors

9 match(es) found. If your search resulted in matches, please click one of those matches to view the corresponding online help page. To return to the results page after viewing a search match, click your browser's back button.

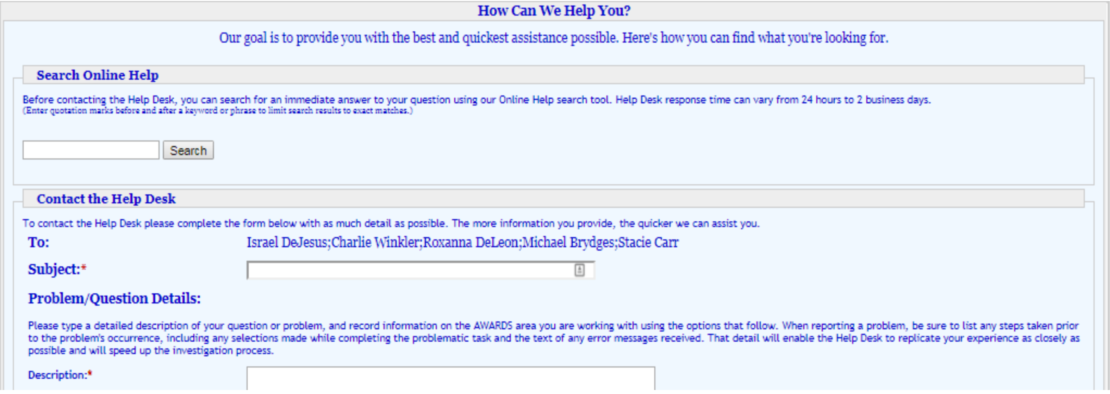
1. - Troubleshooting CSV Validation Errors
After running an HMIS export or validation and upload process, you will receive an export results me...

2. - HMIS Data Standards
This portion of AWARDS Online Help is intended to guide you through functionality specific to the HM...

3. If an Online Help search did NOT resolve your question/issue, close the secondary window containing the search results and click the Help menu found in the top right corner of the screen and select Help Desk.

   PLEASE NOTE: AWARDS users should access the Help Desk within their own AWARDS database and NOT the NYCHMIS AWARDS. Non-AWARDS users having a problem with the NYCHMIS, can access the Help Desk within NYCHMIS.

4. Complete the “How Can We Help You?” page with as much detail as possible. Tickets lacking detail can lead to a longer process to resolve an issue, because our help desk team will need to request additional information. Complete click paths and screen shots are particularly helpful.



How Can We Help You?

Our goal is to provide you with the best and quickest assistance possible. Here's how you can find what you're looking for.

Search Online Help

Before contacting the Help Desk, you can search for an immediate answer to your question using our Online Help search tool. Help Desk response time can vary from 24 hours to 2 business days.
(Enter quotation marks before and after a keyword or phrase to limit search results to exact matches.)

Contact the Help Desk

To contact the Help Desk please complete the form below with as much detail as possible. The more information you provide, the quicker we can assist you.

To: Israel DeJesus;Charlie Winkler;Roxanna DeLeon;Michael Brydges;Stacie Carr

Subject:*

Problem/Question Details:

Please type a detailed description of your question or problem, and record information on the AWARDS area you are working with using the options that follow. When reporting a problem, be sure to list any steps taken prior to the problem's occurrence, including any selections made while completing the problematic task and the text of any error messages received. That detail will enable the Help Desk to replicate your experience as closely as possible and will speed up the investigation process.

Description:*

Please Note: This page can also be opened from within the Messages module directly by using the red and white buoy icon on the left-hand side of the page.

3. Once you've completed your request, click **Send Message.** A copy of your request will be sent to you in the AWARDS Messages module.
4. Periodically check your AWARDS Messages module inbox for a response to your problem report or question. When a response is received, review it carefully. In the event that the Help Desk was unable to investigate with the amount of information provided, you will be asked to supply additional details. Otherwise, you will be provided with information about the area of the application you were working with, or with a resolution to any problem you may have been experiencing.

If you are UNABLE to reach the AWARDS login page: Please contact Foothold Technology at one of the following email addresses:

- helpdesk@footholdtechnology.com (during business hours)
- emergency@footholdtechnology.com (outside of normal office hours)

Foothold Technology's office hours are 9-5 ET M-F, inclusive of all holidays.
The DSS HMIS Team is also available to assist providers with issues related to uploading and data quality.

Section 4:
“Cheat Sheet” for Non-AWARDS Users

“Cheat Sheet” for Non-AWARDS Users on Comma Separated Value (CSV) HMIS Imports/Exports

Prepared by the NYC CCOC Data Management Committee*

Purpose: The Data Management Committee of the New York City Coalition on the Continuum of Care (NYC CCoC) has prepared the instructions below for non-AWARDS users to better understand and troubleshoot issues related to uploading CSV files with HMIS data into the NYC CCoC data warehouse.

A. Database Administrators (DBA) should consult with https://hudhdx.info/Resources/Vendors/5_1_2/HMISCSVSpecifications6_12.pdf for up to date information regarding HMIS CSV Format Specifications v6.12 – September 2018 which includes the following updates:

7/2017	6.1	• Reverted to practice of continuous version numbering for HMIS CSV. • **Geography.csv/2.8 –** added 99 (Unknown/data not collected) to list for *GeographyType*. • **EnrollmentCoC.csv –** corrected reference to DE 3.16 Client Location to use correct DE#. • **Exit.csv/R18:** deleted *CounselingType* and associated list R18.A; added *IndividualCounseling*, *FamilyCounseling*, *GroupCounseling* to accommodate identification of more than one type of counseling received.
9/2017	6.11	Corrections: • **Project.csv** – **HousingType** column was added to file definition in 6.1 but not listed as a change. The column is required. • **Client.csv** – **Race** columns have been non-nullable since 2014 but only a 1/Yes response was defined. Added explicit 0 as the alternative to 1. • **Exit.csv** and **HealthAndDV.csv**: Re-added the **PersonalID** column to both file definitions. The deletion was not intentional; was not listed as a change. • **List 1.4** RecordType for Services.csv: Updated list values consistent with changes listed the file definition and in Appendix C list of changes. • **Appendix C** list of changes for **Inventory.csv**: Struck reference to split of BedType into three separate fields.The change was not needed and was not made in the definition of the Inventory file.
9/2018	6.12	• Updated pagination and table of contents • **Appendix B:** Remove “29:VA:Domiciliary Care” from list 2.6.1 • **Appendix B:** Add “43:HUD:CoC – Youth Homeless Demonstration Program (YHDP) to list 2.6.1 • **Appendix B:** Corrected reference to outdated HMIS Data Standard documentation in Notes • **Services.csv:** Updated hyperlink to List for RecordType 210 to V8.1 • **IncomeBenefits.csv:** Fixed hyperlink to lists 4.4.A; removed list 4.4.A for 4.4.12A OtherInsuranceIdentify • **Exit.csv:** Fixed note for R18.B and R18.2 to say “Integer >0”

B. DBA should make sure that they have all 17 CSV files as follows:

1. Services
2. Affiliation
3. Client
4. Disabilities
5. EmploymentEducation
6. Enrollment
7. EnrollmentCoC
8. Exit
9. Export
10. Funder
11. Geography
12. HealthAndDV
13. IncomeBenefits
14. Inventory
15. Organization
16. Project
17. ProjectCoC

C. If "Affiliation.csv"file has a misspelling alter the first row of for each program that will be imported using Notepad and change the first column from AffiliationID. In AWARDS the correct spelling is used so the DBA may have to make this correction manually each month.

A. Ensure that accepted values are used in the HMIS non-AWARDS system are consistent with HUD data standards use on the frontend and on the backend.

D. When reviewing the Enrollment.CSV file pay special attention to how the HMIS calculates Chronic Homelessness. For additional information use the following URL to gain access to the HMIS Standards Reporting Terminology Glossary: https://www.hudexchange.info/resources/documents/HMIS-Programming-Specifications.pdf.

E. Logic Used to Automate the Chronically Homeless Logic used to identify clients that meet CH criteria: ***Foothold formulation***

i. They must have a Disabling Condition. Disabling condition (3.8) = yes.

ii. They must be Literally Homeless. Living situation (3.917.1) = Code 16, 1, 18 or 27 or [on the night before, did you stay in streets, ES or SH?] (3.917.2c) = yes or [project type] (2.4) = Code 1 or 4 or 8.

iii. They must be experiencing Long Term Homelessness. ([Approximate date started] (3.917.3) <= [project entry date] (3.10) -365 days, OR ([number of times the client has been on the streets, in ES, or SH in the past three years including today] (3.917.4) = "4 or more times" and [total number of months homeless on the street, in ES, or SH in the past three years] (3.917.5) >= "12" or "More than 12 months")

DMC/Anish & Lizzie formulation:
Possible Logic Used to Automate the Chronically Homeless Logic used in HMIS to identify clients that meet criteria:

i. Disabling condition (3.8) = yes or [expected to be of long continued and indefinite duration and substantially impairs ability to live independently] = Yes

ii. Use Code =1) for any of the following: [physical disability] (4.5), [developmental disability] (4.6), [chronic health condition] (4.7), [HIV/AIDS] (4.8), [mental health problem] (4.9), [substance abuse] (4.10), and

iii. Living situation (3.917.1) = Code 16, 1, 18 or 27 or [on the night before, did you stay in streets, ES or SH?] (3.917.2c) = yes or [project type] (2.4) = Code 1 or 4 or 8)

iv. and ([approximate date started] (3.917.3) <= [project entry date] (3.10□365 days or ([regardless of where they stayed last night -- number of times the client has been

v. on the streets, in ES, or SH in the past three years including today] (3.917.4) = code 4 or more times and [total number of months homeless on the street, in ES, or SH in the

vi. past three years] (3.917.5) >= Code 12)

F. Before uploading the CSV files to AWARDS, the DBA should remind program staff to review their data errors or missing data and make corrections as needed. Staff should be given at least 5 days notices to scrub their data prior to the 10th business day of each month as required by DSS for uploads. If the non-AWARDS HMIS system does not have data quality reports, the DBA can send the CSV files to project representatives so they are aware of data errors to ensure the data integrity before uploading!

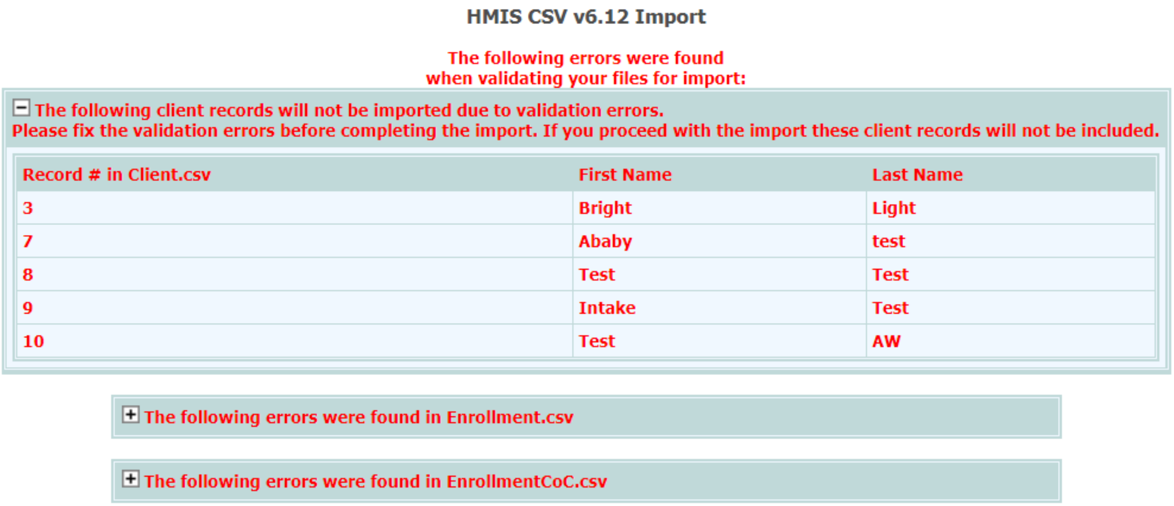
G. Once the CSV files are acceptable, the DBA needs to visit the following URL: https://nychmis.footholdtechnology.com/zf2/ to upload the files to the NYC CoC Data Warehouse.

H. Log-In using the credentials and follow the instructions in Appendix A, Section 2 for how to upload the files

I. If the files are unable to be accepted and have too many errors to pass validation, the DBA must send errors to sites for them to clean up the issues.

J. If validation errors are received, the DBA needs to also consult with their HMIS provider to troubleshoot issues related to HUD HMIS specs and how their CSV files are translated in AWARDS. DBA may also need to speak with DSS HMIS Team and to Foothold to troubleshoot issues as needed.

a. DBA will get a Validation Error Report as part of the import process. The errors will be displayed after the file is selected, after "validate records" is selected, but before the files are imported. Errors will be displayed in the following format:



HMIS CSV v6.12 Import

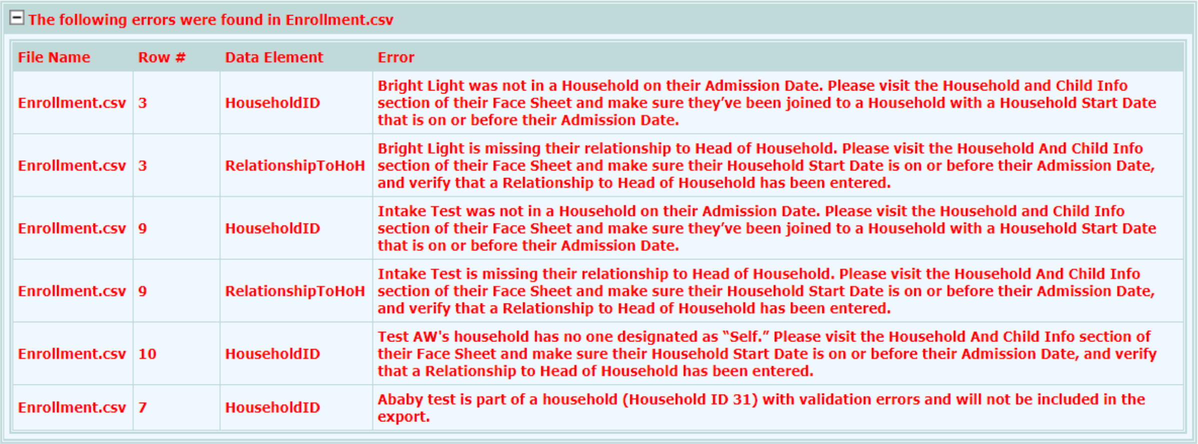
The following errors were found
when validating your files for import:

⊟ The following client records will not be imported due to validation errors.
Please fix the validation errors before completing the import. If you proceed with the import these client records will not be included.

Record # in Client.csv	First Name	Last Name
3	Bright	Light
7	Ababy	test
8	Test	Test
9	Intake	Test
10	Test	AW

⊞ The following errors were found in Enrollment.csv

⊞ The following errors were found in EnrollmentCoC.csv



⊟ The following errors were found in Enrollment.csv

File Name	Row #	Data Element	Error
Enrollment.csv	3	HouseholdID	Bright Light was not in a Household on their Admission Date. Please visit the Household and Child Info section of their Face Sheet and make sure they've been joined to a Household with a Household Start Date that is on or before their Admission Date.
Enrollment.csv	3	RelationshipToHoH	Bright Light is missing their relationship to Head of Household. Please visit the Household And Child Info section of their Face Sheet and make sure their Household Start Date is on or before their Admission Date, and verify that a Relationship to Head of Household has been entered.
Enrollment.csv	9	HouseholdID	Intake Test was not in a Household on their Admission Date. Please visit the Household and Child Info section of their Face Sheet and make sure they've been joined to a Household with a Household Start Date that is on or before their Admission Date.
Enrollment.csv	9	RelationshipToHoH	Intake Test is missing their relationship to Head of Household. Please visit the Household And Child Info section of their Face Sheet and make sure their Household Start Date is on or before their Admission Date, and verify that a Relationship to Head of Household has been entered.
Enrollment.csv	10	HouseholdID	Test AW's household has no one designated as "Self." Please visit the Household And Child Info section of their Face Sheet and make sure their Household Start Date is on or before their Admission Date, and verify that a Relationship to Head of Household has been entered.
Enrollment.csv	7	HouseholdID	Ababy test is part of a household (Household ID 31) with validation errors and will not be included in the export.

b. Once all Errors are corrected the validation error report has less and less errors and the import can be completed.

c. There is also an “importresults.csv” which shows you which clients are uploaded. This will be sent to you after the upload is completed as an attachment to a message labeled “export xxx results.”

K. If validation is passed, copy the message. Do the same if you get any error messages which may occur for documentation purposes to prove that the upload took place and was accepted.

L. The DBA should password protect the client.CSV file [this file has to be converted to EXCEL format before adding a password], along with any error messages which may have occurred, and send them to parties of interest as needed.

M. Data Quality reports can be generated in AWARDS, allowing DBAs to verify if the data uploaded to Foothold was accurately translated. For access to AWARDS contact the DSS HMIS Team.

For additional assistance with the information in this “Cheat-Sheet” please contact:

- Roxanna DeLeon, HMIS Coordinator, NYC DSS HMIS Team, at deleonr@dss.nyc.gov
- Michael Brydges, HMIS Analyst, NYC DSS HMIS Team, at brydgesm@dss.nyc.gov
- Israel DeJesus, HMIS Special Projects, NYC DSS HMIS Team, at dejesusis@dss.nyc.gov

* This document is subject to revision and will be updated over time as new information becomes available. It is current as of the time of this publication. It represents the best knowledge provided by several persons whose agencies do not use the Foothold Technology AWARDS system. NYC DSS and Foothold Technologies do not “certify” the veracity of this document. Users should consider it a guide only that may be helpful. For additional information or assistance, contact the persons listed above.

NYC CCOC | Coalition on the Continuum Of Care

__Appendix B__: Contributing Data Warehouse End User Agreement

This form authorizes NYC HMIS data warehouse access. One form should be completed and submitted to DSS annually for each person requesting access. It should be signed by that person, the agency's executive director, and the NYC HMIS System Administrator.

Contributing HMIS Organization (CHO) Name: ____

Name of Person requesting access: ____

Title of Person requesting access: ______________________________ Email: ___________________________

Requesting access to all or selected projects?
□ All □ Selected (list):____

____

The NYC CCoC recognizes the primacy of client needs in the design and management of the NYC HMIS. These needs include both the need to continually improve and maintain the quality of homeless and housing services with the goal of eliminating homelessness in NYC, as well as the need to maintain client confidentiality and treat the personal data of clients with respect and care.

As the guardians entrusted with this personal data, NYC HMIS Data Warehouse users have a moral and a legal obligation to ensure that the data they upload to the NYC HMIS is being collected, accessed and used appropriately. Proper user training, adherence to the NYC HMIS Policies and Procedures, and a clear understanding of the privacy, security and confidentiality policies are vital to achieving these goals.

Your User ID and Password give you access to the NYC HMIS Data Warehouse. **Sign below to indicate your <u>understanding and acceptance</u> of the proper use of your User ID and password and your intention to comply with all elements of the Homeless Management Information System Data and Technical Standards Notice – published in the Federal Register on July 30, 2004 by the U. S. Department of Housing and Urban Development.** Unauthorized use or disclosure of HMIS information is a serious matter and any Data Warehouse User found to be in breach of the Data Warehouse User Agreement will be subject to the following penalties or sanctions including: the loss or limitation of use of the HMIS and other office technology resources, adverse employment actions including dismissal; and, civil and/or criminal prosecution and penalties.

By signing this form you indicate that you understand and agree to comply with all the statements listed below.

- My NYC HMIS Data Warehouse User ID and Password are for my use only and must not be shared with anyone.
- I will take all reasonable means to keep my User ID and Password physically secure.
- If I am logged into NYC HMIS Data Warehouse and must leave the work area where the computer is located, I **must log-off** of NYC HMIS Data Warehouse before leaving the work area.
- Any computer that has NYC HMIS Data Warehouse "open and running" shall <u>never</u> be left unattended.
- Any computer that is used to access NYC HMIS Data Warehouse must be equipped with locking timeout function.

- Any computer that is used to access NYC HMIS Data Warehouse must have virus protection software installed with auto-update functions.
- Any computer that is used to access NYC HMIS Data Warehouse must have software or hardware firewall protection.
- Failure to log off NYC HMIS Data Warehouse appropriately may result in a breach in client confidentiality and system security.
- If I notice or suspect a security breach, I must notify the HMIS Lead System Administrator – NYC Department of Social Services – within 3 business days.

I affirm the following:

1) I will attend any mandatory NYC HMIS trainings offered on privacy, data collection, and security policies.

2) I have read and will abide by all policies and procedures in the NYC HMIS Policies and Procedures and have adequate training and knowledge to upload to and export data from and/or run reports from the NYC HMIS Data Warehouse.

3) I will maintain the confidentiality of client data in the NYC HMIS Data Warehouse as outlined above and in the NYC HMIS Policies and Procedures Manual.

4) I will only search, view, or upload data to the NYC HMIS Data Warehouse that is relevant to the delivery of services to people in housing crisis in New York City.

To be completed by the contributing organization:

____ _______________

Person requesting NYC HMIS Data Warehouse access Date

____ _______________

CHO HMIS System Administrator or Executing Officer (CHO’s Executive Director) Date

To be completed by DSS:

____ _______________

NYC HMIS Data Warehouse System Administrator or Designee Date

NYC CCOC Coalition on the Continuum Of Care

Appendix C: CHO NYC HMIS Participation Agreement

This form must be completed and signed by each Contributing HMIS Organization and submitted to DSS annually.

by and between
New York City Department of Social Services
and
Contributing HMIS Organization (CHO) Name: ____

THIS HOMELESS MANAGEMENT INFORMATION SYSTEM ORGANIZATION PARTICIPATION AGREEMENT (the “Agreement”) is made by and between the New York City Department of Social Services (DSS), as the primary coordinating entity for the New York City Coalition on the Continuum of Care Homeless Management Information System (hereinafter “NYC HMIS”), and____, a nonprofit corporation or organization located at ____ (hereinafter “Organization”).

Whereas, the NYC HMIS is a client information system that records the use of housing and services which can use to determine the utilization of services of participating agencies, identifying gaps in the local service continuum and develop outcome measurements.

Whereas, DSS, in partnership with New York City Continuum of Care, is the Lead Agency for the NYC HMIS.

Now, therefore, in consideration of the mutual promises contained in this Agreement, DSS and Organization agree as follows:

I. Definitions

“Organization” is the Organization named in this Agreement.

“Client” is a consumer of services provided by or through the Organization.

“Contributing HMIS Organizations (CHO)” are all the Agencies participating in NYC HMIS.

“Data Warehouse” is the central repository of client level data from the CHOs.

“Participating Project” means a project operated by a Contributing HMIS Organization (CHO) which records data elements regarding clients served and uploads these data elements through agreed upon means to the Data Warehouse operated by the Lead HMIS Agency.

“Project-level HMIS-compliant system” is defined as a client management information system operated by a project that allows the project to collect the minimum required data elements and to meet other established minimum participation thresholds as set forth in CHO HMIS Participation Agreements.

II. Conditions for NYC HMIS Participation

The Organization agrees to abide by the most current NYC CCoC HMIS Policies and Procedures approved and adopted by the NYC CCoC, incorporated by reference, except as stated in **Section III. Exceptions**. These include: privacy, security, client consent and data entry requirements. The Organization also agrees to assure that all employees and agents comply with these policies. The "New York City CCoC HMIS Policies and Procedures" can be obtained online at www.nychomeless.com.

The Organization indicates cooperation with the NYC CCoC HMIS Policies and Procedures for all participating projects through annual certified compliance with the Administrative and Software Certification Checklist, attached hereto as **Appendix D. Administrative and Software Certification Checklist** and incorporated by reference, and Annual Security Certification Checklist or certification of no change, attached hereto **as Appendix E. Security Certification Checklist** and incorporated by reference. A list of participating projects for the Organization is provided in Appendix D.

The Organization shall appoint a CHO HMIS Administrator responsible for all duties specified in Appendix D. The Organization shall appoint a CHO HMIS Security Contact responsible for all duties specified in Appendix E.

III. Exceptions

Organization has indicated in Appendix D or E of this Agreement that it does not, at the time of execution of this Agreement, meet all requirements for participation in the NYC HMIS. Consistent with NYC CCoC Policies and Procedures, Organization shall resolve the issues not later than the date(s) indicated in Appendix D and E and shall re-submit an updated Appendix D and/or E, as applicable.

IV. Rights and Responsibilities of Parties

As stated in the Memorandum of Understanding (MOU), as the Lead HMIS Agency, DSS has the following responsibilities:

a) Governance and Reporting
b) Planning and Policy Development
c) Grant Administration
d) HMIS Lead System Administration
e) End User Administration
f) Data Quality and Compliance Monitoring
g) Conducting Security, Privacy and Data Quality trainings
h) Ensuring HMIS is operating in accordance with these Policies and Procedures

CHOs are responsible for:

a) Self-certifying compliance with these policies and procedures
b) Remediation for non-compliant systems
c) Collecting and uploading data to the NYC HMIS as per these policies and procedures
d) Ensuring End Users of the project level HMIS compliant system are adhering to the privacy and confidentiality requirements
e) Training CHO End Users on CHO's Project-level HMIS-compliant system
f) Notifying DSS within 15 days if any HMIS data warehouse end user needs to be deactivated.

V. Oversight and Sanctions

The HMIS Lead Agency will monitor CHO compliance with these policies and procedures and can verify CHO self-certifications via site visits.

VI. Other Terms and Conditions

DSS shall not be liable to the Organization for any services, hardware, or software associated with the operation of any project-level HMIS-compliant system except as specified above.

DSS shall not be liable to Organization for any cessation, delay, or interruption of any Data Warehouse services, nor for any malfunction of Data Warehouse software.

This Agreement shall be in force from the execution date for a period of one year or until terminated in writing by either party. Without limiting the generality of the foregoing or the right of DSS to terminate this Agreement for any reason, DSS may terminate this Agreement if funding for HMIS or any part thereof becomes unavailable or is restricted.

IN WITNESS WHEREOF, DSS and Organization have executed this Agreement by their respective duly authorized representatives.

NYC Department of Social Services (DSS)

By: ___________________________________ Title: ___________________________ Date: _________

ORGANIZATION: _______________________________________

[Insert Organization name]

By: ____________________________________ Date ________

Printed Name: ____________________________________

Title or Capacity: ____________________________________

NYC HMIS Rev. 10/16/2019

NYC CCOC Coalition on the Continuum Of Care

One Appendix D form must be completed, signed and submitted to DSS annually by each Contributing HMIS Organization (CHO). It provides DSS with information on information on key CHO contacts and CHO HMIS software and certifies CHO compliance with administrative, technical, and security responsibilities and requirements.

<u>Appendix D</u>*: *NYC HMIS Administrative, Software Certification and Security Checklists

Contributing HMIS Organization (CHO) Name: ____

A. Identification and Contact Information

You are required to notify DSS within 15 business days if one of these contacts changes.

Executing Officer (Executive Director or Chief Executive Officer)

a. Name ____

b. Title ____

c. Phone ____

d. Email ____

CHO HMIS Administrator (may be the same as the Executing Officer)

a. Name ____

b. Title ____

c. Phone ____

d. Email ____

Backup CHO HMIS Administrator

a. Name ____

b. Title ____

c. Phone ____

d. Email ____

CHO Security Contact

a. Name ____

b. Title ____

c. Phone ____

d. Email ____

B. Is AWARDS software used as the CHO's project-level HMIS-compliant database?

□ Yes

□ No. If no, identify the software and version in use for collecting HMIS information:

____

You are required to notify DSS and Foothold Technology in advance of any changes in this software.

C. Key Responsibilities

CHO HMIS Administrator’s duties include:

- Providing a single point of communication between the CHO End Users and the HMIS Lead around HMIS issues;
- Ensuring the stability of the CHO connection to the Internet and the data warehouse, either directly or in communication with other technical professionals;
- Maintaining awareness of industry standards;
- Training CHO End-Users in data collection, security and privacy policies and procedures, and assuring End Users receive any requisite training provided by HMIS Lead for End Users;
- Providing support for generating organization reports;
- Managing CHO user names and passwords for project level HMIS compliant system;
- Monitoring compliance with standards of client confidentiality and data collection, entry, and retrieval; and
- Participating in CHO HMIS training.

Security Contact duties include, but are not limited to:

- Annually review the Section E of this appendix, Assurances of Consistency with Security Plan
- Security Certification Checklist document, test the CHO security practices for compliance, and work with appropriate vendors (where applicable) to confirm security compliance of the project-level HMIS-compliant system;
- Using this Security Certification Checklist document, certify that the CHO adheres to the Security Plan or provide a plan for remediation of non-compliant systems, including milestones to demonstrate elimination of the shortfall over time;
- Communicate any security questions, requests, or security breaches to the DSS System Administrator and/or DSS Security Officer;
- Communicate security-related HMIS information to the CHO’s End Users;
- Complete any CoC-mandated security training offered by the HMIS Lead; and
- Additional duties as specified in the HMIS Participation Agreement.

D. Assurances of Consistency with Policies and Procedures

Each CHO is required to establish and follow the following policies and practices. If the requirement cannot be met at the time of execution of the Participation Agreement, you must indicate a date not later than three months execution date by which you will have met the requirement. At that time, you will be required to submit an updated version of this form demonstrating your compliance**. <u>If you achieved full compliance last year and maintain such compliance to date, you may skip this checklist and sign below.</u>**

Administrative and Software Certification Checklist			
#	Required Policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
I	**Administrative Requirements**		
1	CHO has a policy detailing its internal communication practices for HMIS matters consistent with **Section 3.2.4 CHO Communications** of the NYC HMIS policies and procedures.		
2	CHO has a policy for granting access to its project-level HMIS-compliant system's End Users consistent with **Section 3.6.1 User Levels and Activation** of the policies and procedures.		
3	The CHO has adopted the minimal End User Agreement provided by the NYC HMIS Lead		
3.1	If not, CHO's End User Agreement otherwise meets the minimum requirements established in **Section 3.6.2 CHO User Agreement** of the policies and procedures.		
4	CHO End User Agreements are signed and on file for all staff who access the project-level HMIS-compliant system. See Appendix G.		
5	CHO has a policy for managing the breach of End User Agreement that meets the minimum standards outlined in **Section 3.6.3 User Agreement Breach** of the policies and procedures.		
6	Each CHO End User has been trained on system use, privacy, security, and data collection requirements consistent with training sessions provided by the HMIS lead and the NYC HMIS policies and procedures, consistent with **Section 3.7 Training Requirements** of the policies and procedures.		
7	The CHO has adopted the minimal standard Privacy Policy provided by the NYC HMIS Lead		
7.1	If not, CHO's Privacy Policy otherwise meets the minimum requirements established in **Section 6. Privacy Policy** of the policies and procedures.		
8	The CHO's Privacy Policy is posted on the CHO's website.		
9	A sign including the required language described in **Section 6.6.2 Informed Client Consent** of the policies and procedures is posted at all intake desks or other location where data collection occurs.		

Administrative and Software Certification Checklist			
#	Required Policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
10	The CHO has a policy requiring that all client data is entered into the system as per the requirements of the data collection point, and for "update " within, at most, three business days of a client interaction, consistent with **Section 7.4.1 Timeliness.**		
10.1	The CHO has a policy for conducting logic checks to validate the accuracy of the data in its project-level HMIS-compliant system and regularly comparing universal and program specific data elements to available paper records and updating/correcting missing or inaccurate data, consistent with **Section 7.4.3 Accuracy** of the policies and procedures.		
II	**Software and Technical Requirements**		
1	CHO's project-level HMIS compliant client data collection system is a relational database capable of recording client data from a limitless number of service transactions and preserving all required historical data as outlined in **Section 7. Data Quality Plan** of the NYC HMIS policies and procedures and the current HUD HMIS Data Standards.		
2	System has the capacity to collect data on system use for the purposes of data quality and security, including login attempts, search parameters, and incidents of changes made to records.		
3	System has the capacity to collect all project descriptor, universal, program-specific, and metadata elements as specified in **Section 7. Data Quality Plan** of the policies and procedures.		
4	System has the capacity to meet technical security requirements specified in **Section 4. HMIS Security Plan** of the policies and procedures and technical privacy requirements specified in **Section 6. Privacy Policy** of the policies and procedures.		
5	System has the capacity to transfer data directly to the Data Warehouse or export a CSV file of all required data elements consistent with current HUD HMIS CSV Format documentation for the purposes of upload to the Data Warehouse.		

If the software used for data collection changes, DSS and Foothold Technology must be notified in advance.

E. Assurances of Consistency with Security Plan

Each CHO is required to meet the following security requirements. If the requirement cannot be met at the time of execution of the Participation Agreement, you must indicate a date not later than three months execution date by which you will have met the requirement. At that time, you will be required to submit an updated version of this form demonstrating your compliance. **<u>If you achieved full compliance last year and maintain such compliance to date, you may skip this checklist and sign below.</u>**

Security Checklist			
#	Required policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
1	CHO has a policy regarding conducting background checks and hiring individuals with criminal justice histories consistent with **Section 4.4.1 Criminal Background Verification** of the HMIS policies and procedures.		
2	Documentation is on file that each End User has completed security training prior to gaining system access consistent with **Section 4.4.2 Annual Security Training** of the HMIS policies and procedures.		
3	CHO has established procedures protecting the physical security of the facilities and media in which the data is stored or has provisions in its contract with the provider of the project-level HMIS-compliant system to meet the minimum standards established in **Section 4.6.1 Physical Security** of the policies and procedures (including temperature control and surge suppressors).		
4	All HMIS data is copied to another medium and stored in a secure off-site location at least weekly or the CHO has included provisions in its contract with the provider of the project-level HMIS-compliant system to meet the minimum standards established in **Section 4.6.2 Backup** of the policies and procedures.		
5	Restoration of backed-up data has been tested within the last 12 months.		
6	CHO has policies and procedures that specify how the software provider or system operator will address all reported bugs within three business days and specify that, if customer intervention is required, the CHO is responsible for ensuring that all enhancements, upgrades and bug fixes are applied promptly upon release by the software provider, consistent with **Section 4.6.3 Software Security** of the policies and procedures.		

Security Checklist

#	Required policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
7	CHO maintains and follows procedures to install, update and use anti-virus software on all CHO-owned devices used to access the project-level HMIS-compliant system, consistent with **Section 4.6.3 Software Security** of the policies and procedures.		
7.1	Identify the anti-virus software in use		
7.2	Specify the frequency with which the software is updated and the frequency with which the devices will be scanned. At minimum, update of the software and scan the relevant devices for viruses and malware must be done monthly		
8	CHO has established procedures for protecting HMIS data behind a firewall or has provisions in its contract with the provider of the project-level HMIS-compliant system to meet the minimum standards established in **Section 4.6.4 Boundary Protection** of the policies and procedures.		
9	The project-level HMIS-compliant system's password requirements have been tested within the last 12 months and meet the minimum standards established in **Section 4.6.5 System Access User Authentication and Passwords** of the policies and procedures.		
10	The following username protections have been formalized in a written procedure and tested within the last 12 months:		
10.1	Defines a period of inactivity after which the user's workstation must be automatically logged out of the system and/or locked out of the computer, requiring a username and password to resume use of the project-level HMIS-compliant system.		
10.2	Requires that any default passwords provided for initial entry into the application be changed on first use.		
10.3	Defines how individual users' forgotten passwords will be reset and communicated to the user.		
10.4	Specifies how unsuccessful login attempts will be handled and confirm that the project-level HMIS-compliant system will maintain an auditable record of all attempted logins. At maximum, 5 consecutive unsuccessful login attempts must lock a user out of the system for at least 30 minutes.		
11	CHO has a procedure for accessing its project-level HMIS-compliant system through networks and devices not owned or managed by the CHO consistent with **Section 4.6.5 System Access User Authentication and Passwords** of the policies and procedures.		
12	CHO's project-level HMIS-compliant system maintains audit records of user activity, including attempted logins, searches conducted by each user, records altered by each user, and records added by each user.		
13	CHO has a policy to monitor audit records regularly for security breaches at least monthly, consistent with **Section 4.6.6 Audit Controls** of the policies and procedures.		

Security Checklist			
#	Required policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
14	CHO has a policy specifying that End Users may not electronically transmit any unencrypted client-level data across a public network, consistent with requirements associated with Personally Identifying Information (PII) described in **Section 4.7 PII Management and Disposal** of the policies and procedures.		
15	CHO has a policy specifying any hard drives or removable media on which PII is stored will be encrypted and that users are prohibited from storing client-level data on any personally owned media, consistent with **Section 4.7 PII Management and Disposal** of the policies and procedures.		
16	CHO has a policy describing how hard-copy and electronic client-level data will be protected and disposed of, consistent with **Section 4.7 PII Management and Disposal** of the policies and procedures and industry standards for digital media disposal.		
17	CHO has a policy specifying the thresholds and process for security incident reporting, consistent with **Section 4.8 Security Incidents** of the policies and procedures.		
18	CHO maintains records of any and all security breaches to the project-level HMIS-compliant system.		
19	Each CHO will have a plan in place for maintaining and recovering access to its own data, consistent with **Section 5** Disaster Recovery of the policies and procedures.		

We affirm and certify that this organization, ____ ______________________________, achieved full compliance last year (and has a completed checklist on file with DSS) for all requirements listed as “CHO” (Contributing HMIS Organization) responsibilities in the U.S. Department of Housing and Urban Development Homeless Management Information System (HMIS) Data and Technical Standards Final Notice and with the NYC CCoC HMIS Policies and Procedures. This certification is incorporated into the HMIS Participation Agreement. Any misrepresentation of the foregoing may result in termination of the Participation Agreement.

OR

We affirm and certify the above information is true and that this organization, ___________________________ ____, is in full compliance with all requirements listed as “CHO” (Contributing HMIS Organization) responsibilities in the U.S. Department of Housing and Urban Development Homeless Management Information System (HMIS) Data and Technical Standards Final Notice and with the NYC CCoC HMIS Policies and Procedures or will be in compliance within the timeframes stated above. This certification is incorporated into the HMIS Participation Agreement. Any misrepresentation of the foregoing may result in termination of the Participation Agreement.

CHO HMIS System Administrator

Signature ____

Date ____

Printed Name ____

Title ____

CHO HMIS Security Contact

Signature ____

Date ____

Printed Name ____

Title ____

Executing Officer (Executive Director or Chief Executive Officer)

Signature ____

Date ____

Printed Name ____

Title ____

NYC CCOC Coalition on the Continuum Of Care

Appendix E: Project List

One Appendix E must be completed and submitted to DSS annually by each Contributing HMIS Organization (CHO).

Provide a list of all projects operated by this organization with a primary purpose of meeting the specific needs of people who are homeless, at-risk of homelessness or formerly homeless, whether or not the project participates in HMIS. (For projects that do upload client data to HMIS, one Appendix F form is needed per project.)

Project types include:

Coordinated Assessment
Day Shelter
Emergency Shelter
Homelessness Prevention

Transitional Housing
Permanent Supportive Housing
PH – Housing with Services
PH – Housing Only

Rapid Re-housing
Safe Haven
Services Only
Street Outreach

TH-RRH
Other

List all of your organization's projects that are dedicated to serving homeless or formerly homeless persons, regardless of funding source and regardless of whether or not they upload to HMIS. This must include all projects reflected in the Housing Inventory Count (HIC).

Project Name	Project Type	CHO uploads client data to HMIS data warehouse? (Yes or No)	CoC Funded? (Yes or No)	# Beds	In DHS CARES or StreetSmart? (Yes or No)
ADD ADDITIONAL ROWS IF NEEDED					

Project Name	Project Type	CHO uploads client data to HMIS data warehouse? (Yes or No)	CoC Funded? (Yes or No)	# Beds	In DHS CARES or StreetSmart? (Yes or No)

Appendix F: NYC HMIS Project Information Form

One form must be completed for each HMIS-participating project and submitted to DSS prior to initial upload, when there are changes to any Project F information, and on an annual basis thereafter.

For consolidated projects or other projects that are organized as smaller constituent projects in the NYC HMIS data warehouse, one Appendix F form must be completed for each of the constituent projects.

For TH-RRH projects, HUD requires that they are set up as two distinct projects in HMIS; submit separate Appendix F forms for the TH and RRH components of your project.

Projects must split into two separate projects if only a portion of the clients are being uploaded; contact DSS and Foothold Technology for further clarification and/or assistance.

Organization Name	
Project Name (as per NYC HMIS)	
Project Name (as per Grant/GIW)	
Contract Grant #	
Is this a consolidated project?	□ Yes □ No If yes, provide HMIS project names for all projects in the consolidation: ____________________ ____________________

Project Address 1*	
Project Address 2*	
Project City*	
Project State	
Project Zip Code	
Project County	
Contact Person	
Contact Email	
Contact Phone #	
Include contact in HMIS e-list?	□ Yes □ No

* If project is a victim services provider, provide zip code but do not disclose address or city.

1. **Is this project dedicated to serving homeless and formerly homeless persons?**

   □ Yes
   □ No

   1a. If no, is a portion of the project dedicated to serving homeless or formerly homeless persons?

   □ Yes
   □ No

2. **Does this project upload client data to HMIS?**
   □ Yes
   □ No

3. **If this program does not upload into HMIS, is it because this program a victim services provider?**
   □ Yes
   □ No

4. **If this project uploads client data to HMIS, is information included on all current clients in the project?**
   □ Yes
   □ No

5. **Project Type:** (check ONLY ONE - Each project type is distinct and requires separate HMIS set-up. A project that has multiple types should complete multiple forms and only select one type per form/set-up. If you have more than one project type at your site (e.g. HUD TH and SAMHSA PATH), you must create separate projects in HMIS and upload separately for each project.)
   □ Coordinated Assessment
   □ Day Shelter
   □ Homelessness Prevention
   □ Other (specify: ______________________________)
   □ PH – Housing Only
   □ PH – Housing with Services (no disability required for entry)
   □ PH – Permanent Supportive Housing (disability required for entry)
   □ PH – Rapid-Re-Housing
   □ Safe Haven
   □ Services Only
   □ Street Outreach
   □ Transitional Housing
   □ Emergency Shelter
      If this project is an Emergency Shelter project, indicate method of tracking ES utilization:
         □ Entry/Exit Method
         □ Night-by-Night Method

6. Federal Partner Funding Source: (check all that apply and complete columns to the right)

Federal Partner Programs & Components	***Original Grant Start Date**** *MM/DD/YYYY*	***Terminating Grant End Date***** *MM/DD/YYYY*	***Grant Number*** *(first 6 digits)*
HUD: COC			
□ HUD:CoC – Permanent Supportive Housing			
□ HUD:CoC – Rapid Re-Housing			
□ HUD:CoC – Supportive Services Only			
□ HUD:CoC – Transitional Housing			
□ HUD:CoC – Safe Haven			
□ HUD:CoC – Single Room Occupancy (SRO)			
□ HUD:CoC – Youth Homeless Demonstration Program (YHDP)			
□ HUD:CoC – Legacy funding: Shelter Plus Care (S+C)			
□ HUD:CoC – Legacy funding: Section 8 Moderate Rehab SRO			
□ HUD:CoC – Legacy funding: Supportive Housing Program (SHP)			
HUD: ESG			
□ HUD:ESG – Emergency Shelter (operating and/or essential services)			
□ HUD:ESG – Homelessness Prevention			
□ HUD:ESG – Rapid Rehousing			
□ HUD:ESG – Street Outreach			
HUD: HOPWA			
□ HUD:HOPWA – Hotel/Motel Vouchers			
□ HUD:HOPWA – Housing Information			
□ HUD:HOPWA – Permanent Housing (facility based or TBRA)			
□ HUD:HOPWA – Permanent Housing Placement			
□ HUD:HOPWA – Short-Term Rent, Mortgage, Utility assistance			
□ HUD:HOPWA – Short-Term Supportive Facility			
□ HUD:HOPWA – Transitional Housing (facility based or TBRA)			
HUD/VASH			
□ HUD:HUD/VASH			
HHS: PATH and HHS: RHY			
□ HHS:PATH – Street Outreach & Supportive Services Only			
□ HHS:RHY – Basic Center Program (prevention and shelter)			
□ HHS:RHY – Maternity Group Home for Pregnant and Parenting Youth			
□ HHS:RHY – Transitional Living Program			
□ HHS:RHY – Street Outreach Project			
□ HHS:RHY – Demonstration Project			

*If this grant has been renewed, provide original grant start date.

** If grant is expected to be renewed, leave grant end date blank.

Federal funding sources continue on next page

Federal Partner Funding Source: (check all that apply and complete columns to the right) *continued*

Federal Partner Programs & Components	***Original Grant Start Date**** *MM/DD/YYYY*	***Grant End Date***** *MM/DD/YYYY* *(if terminating)*	***Grant Number*** *(first 6 digits)*
VA			
□ VA: CRS Contract Residential Services			
□ VA: Community Contract Safe Haven Program			
□ VA: Compensated Work Therapy Transitional Residence			
□ VA: Supportive Services for Veteran Families			
□ VA: Grant Per Diem — Bridge Housing			
□ VA: Grant Per Diem — Low Demand			
□ VA: Grant Per Diem — Hospital to Housing			
□ VA: Grant Per Diem — Clinical Treatment			
□ VA: Grant Per Diem — Service Intensive Transitional Housing			
□ VA: Grant Per Diem — Transition in Place			
N/A			
□ N/A: Other Federal funding. Specify: _______________			

*If this grant has been renewed, provide original grant start date.

** If grant is expected to be renewed, leave grant end date blank.

7. **Which of the following other sources of funding does this project receive?** (Check as many as apply).

□ NY/NY 1 or 2

□ NY/NY 3

□ NYC 15/15

□ DHS SRO Support Subsidy

□ DOHMH

□ HASA

□ High Needs 1 or High Needs 2

□ MRT

□ OMH

□ OASAS

□ SHFYA

□ Other (specify:___________________)

8. **Bed and Unit Inventory Information:**

The inventory associated with the clients that are uploaded to the HMIS data warehouse must be listed as both beds and units. (If you use entitlement filters to upload a portion of your client data to HMIS, do not report here for the inventory associated with non-uploaded clients.)

- Units must be consistent with the household-level capacity for which this project is funded; if it houses single adults, each adult should be counted as his or her own household.
- Beds must be consistent with the person-level capacity for which this project is funded.
- Examples:
  - For projects serving single adults (i.e., a family of one), the counts of both units (household-level) and beds (person-level) typically match the number of persons.
  - For projects serving families with children, the count of units (household-level) typically matches the number of families; the count of beds (person-level) typically matches the number of persons.
  - For projects leasing to multiple households in within a larger apartment (e.g., 1 physical apartment with 3 rooms each leased to a person), the unit count is consistent with the number of households (including single-person households), and the bed count is consistent with the number of individuals.

	Count (Apartments or Units or Beds)
Physical apartments	
HOUSEHOLD/UNIT Inventory	
PERSON/BED Inventory	

9. **How would you describe the site where your housing units are located or your service encounters are provided?** (check only one)

□ Site-based – single site
□ Site-based – clustered/multiple sites
□ Tenant-based – scattered site

10. **Which of the following target populations best describes the clients served by this project?** A population is considered a target population if the project is intended to serve that population and at least 75% of the clients served by the project fit that description. (check only one)

□ SM Single Males age 18 years and up
□ SF Single Females age 18 and over
□ SMF Single Male and Females age 18 and up
□ CO Couples Only, No Children
□ HC Households with Children
□ SMHC Single Males age 18 years and up and Households with Children

□ SFHC Single Females age 18 and up and Households with Children
□ SMF+HC Single Males and Females age 18 and up plus Households with Children
□ YM Youth Males under 25 years old
□ YF Youth Females under 25 years old
□ YMF Youth Males Females under age 25

11. **Does this project have any of the following "target populations"?** (if applicable, check only one).

A population is considered a target population if the project is designed to serve that population and at least three-fourths of the clients served by the project fit the description.

□ Domestic violence victims
□ Veterans

□ People with HIV/AIDS
□ Not Applicable

12. **When did your organization start operating this project (month/day/year)?** ______/_____/________

NYC CCOC Coalition on the Continuum Of Care

Appendix G: SAMPLE NYC HMIS Project End User Agreement

CHOs are responsible for having all end users of their project-level HMIS compliant home system annually complete and sign an agreement such as this. These agreements must be kept on file by the CHO. End user is defined as any individual that enters or accesses information in the project-level HMIS compliant home system.

End User: ____(print full name)

End User's title: ____

End User's work phone number: ____

End User's work e-mail: ____

Project(s): ____

Organization: ____

USER POLICY

HMIS Project End Users will comply, to the best of their ability, both with the policies and procedures of their organization and the NYC CCoC HMIS policies and procedures. As guardians entrusted with personal data, [_________________________________] users have a moral and a legal obligation to ensure that the data they

organization name

collect is being collected, accessed and used appropriately, as well as a duty to protect client information. It is also the responsibility of each user to ensure that client data is only used to the ends to which it was collected. Proper user training, adherence to the NYC CCoC Policies and Procedures, and a clear understanding of client confidentiality are vital to achieving these goals.

USER RESPONSIBILITY

Your User ID and Password give you access to [name of project level HMIS compliant system] and data. By signing this form below you indicate your understanding and acceptance of the proper use of this access. Failure to uphold the confidentiality standards set forth below is grounds for immediate termination from the system.

Please initial before each bullet point to indicate you have read each statement, understand, and agree.

_____ I understand that each client must be made aware of the CHO's privacy policy (the "Privacy Policy") and its content regarding the collection, use and maintenance of such client's protected personally identifiable information.

_____ I understand that the Privacy Policy must be provided to the client upon request and a notice indicating that the Privacy Policy is available must be posted at the provider's intake desk.

_____ I understand that my User ID and Password are for my use only and will not be shared with anyone.

_____ I will take all reasonable precautions to keep my Password physically secure.

_____ I will never let anyone else know my password, use my Password, or access the system using my password.

_____ I will only let only individuals who are authorized view information in the system (or the Client to whom the information pertains).

_____ I will only view, obtain, disclose, or use the database information that is necessary to perform my job.

_____ I will not leave a computer unattended when I am logged into the system.
_____ I will log-off the system before leaving the work area, even for a very short time.
_____ I understand that failure to log off [name of system] appropriately may result in a breach in client confidentiality.
_____ I will assure that any and all printouts / hard copies of client information must be kept in a secure place, such as a locked file.
_____ I will assure that any printouts / hard copies of client information no longer needed will be shredded or otherwise properly destroyed to maintain confidentiality.
_____ If I notice or suspect a security breach, I will immediately notify my organization HMIS security contact, [name].

I affirm the following:

_____ I have received training in how to use [name of system].
_____ I have will abide by all policies and procedures in the NYC CCoC HMIS Policies and Procedures and have adequate training and knowledge to enter data.
_____ I will maintain the confidentiality of client data as specified in the NYC CCoC HMIS Policies and Procedures.
_____ I will only collect, enter and extract data in [name of system] that is relevant to the delivery of services to persons in the homeless assistance system in New York City.

I, (**Print**) ____, acknowledge that I have received the NYC HMIS Policies and Procedures. I understand and agree to comply with the requirements contained in the Policies and Procedures. I further understand that failure to comply with the Policies and Procedures may result in sanctions, up to and including termination and civil and criminal penalties.

I understand and agree to comply with all the statements listed above.

____
CHO Project End User Signature   Date

____
CHO Supervisor Signature   Date

____
Supervisor's printed name   Supervisor's title

NYC CCOC Coalition on the Continuum Of Care

Appendix H: SAMPLE Minimal Standard CHO Privacy Policy

Your organization must have a privacy policy with these minimal standards in place. It should be provided to all end-users at your organization prior to their completion of the Project End User Agreement (see Appendix G). Organizations must provide a point of contact for complaints and accountability (see #1 under Complaints and Accountability).

Privacy Policy for ____
(Organization Name)

What this Policy Covers.

1. This document describes the privacy policy and practices of _______________. Our main office is at ______________________________________.
2. This policy covers the collection, use, and maintenance of protected personal information for clients of __________________________, as an organization affiliated with the NYC Coalition on the Continuum of Care (CCoC).
3. Personally Identifiable Information/ Protected Identifying Information (PII) is any personal information we maintain about a client that:
    a. Allows identification of an individual directly or indirectly;
    b. Can be manipulated by a reasonably foreseeable method to identify a specific individual; or
    c. Can be linked with other available information to identify a specific client.
4. We adopted this policy because the Department of Housing and Urban Development issued standards for Homeless Management Information Systems. We intend our policy and practices to be consistent with those standards. See 69 Federal Register 45888 (July 30, 2004).
5. This policy informs our clients, our staff, and others how we process personal information. We follow the policy and practices described in this privacy policy.
6. We may amend our policy or practices at any time. Amendments may affect PII that we obtained before the effective date of the amendment.
7. We give a written copy of this privacy policy to any individual who asks for it.
8. We maintain a copy of this policy on our website at __________________

How and Why We Collect PII.

1. We collect PII only when appropriate to provide services or for another specific purpose of our organization or when required by law. We may collect information for these purposes:
    a. To provide individual case management;
    b. To produce aggregate-level reports regarding use of services;
    c. To track individual project-level outcomes;
    d. To identify unfilled service needs and plan for the provision of new services;
    e. To conduct research for consulting and/or educational purposes; and
    f. To accomplish any and all other purposes deemed appropriate by the CCoC.

2. We only use lawful and fair means to collect PII.
3. We normally collect with the knowledge or consent of our clients. If you seek our assistance and provide us with PII, we assume that you consent to the collection of information described in this policy.
4. We share this data with the NYC Department of Social Services (DSS), Federal Homeless Policy and Reporting unit (FHPR) a/k/a/ the "HUD CoC unit": the agency appointed by the CCoC to manage all PII we record about our clients. This agency is required to maintain the confidentiality of the data.
5. We post a sign at our intake desk or other location explaining the reasons we ask for PII. The sign says:

   ____

   ____

   ____

   [SAMPLE LANGUAGE; CHOs SHOULD REPLACE THIS LANGUAGE WITH THEIR OWN, AS APPROPRIATE] <*We collect personal information about homeless individuals in a computer system called a Homeless Management Information System (HMIS) for reasons that are discussed in our privacy policy. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless individuals, and to better understand the needs of homeless individuals. We only collect information that we consider to be appropriate. If you have any questions or would like to see our privacy policy, our staff will provide you with a copy.*>

<u>How We Use and Disclose PII</u>.

1. We use or disclose PII for activities described in this part of the policy. We may or may not make any of these uses or disclosures of your PII. We assume that you consent to the use or disclosure of your PII for the purposes described below and for other uses and disclosures that we determine to be compatible with these uses or disclosures:
   a. To provide or coordinate services to individuals;
   b. for functions related to payment or reimbursement for services;
   c. To carry out administrative functions such as legal, audits, personnel, oversight and management functions;
   d. To create de-identified (anonymous) information;
   e. When required by law to the extent that use or disclosure complies with and is limited to the requirements of the law;
   f. To avert a serious threat to health or safety if:
      i. We believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and
      ii. The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.
   g. To report about an individual we reasonably believe to be a victim of abuse, neglect or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence in any of the following three circumstances:
      i. Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;

ii. If the individual agrees to the disclosure; or

iii. To the extent that the disclosure is expressly authorized by statute or regulation and either of the following are applicable:

A. We believe the disclosure is necessary to prevent serious harm to the individual or other potential victims; or

B. If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PII for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure;

iv. When we make a permitted disclosure about a victim of abuse neglect or domestic violence, we will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:

A. We, in the exercise of professional judgment, believe informing the individual would place the individual at risk of serious harm; or

B. We would be informing a personal representative (such as a family member or friend), and we reasonably believe the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as we determine in the exercise of our professional judgment.

h. To a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:

i. In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;

ii. If the law enforcement official makes a written request for PII that:

A. Is signed by a supervisory official of the law enforcement agency seeking the PII;

B. States that the information is relevant and material to a legitimate law enforcement investigation;

C. Identifies the PII sought;

D. Is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

E. States that de-identified information could not be used to accomplish the purpose of the disclosure.

iii. If we believe in good faith that the PII constitutes evidence of criminal conduct that occurred on our premises;

iv. In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PII disclosed consists only of name, address, date of birth, place of birth, social security number and distinguishing physical characteristics; or if:

A. The official is an authorized federal official seeking PII for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others); and

B. The information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

i. To comply with government reporting obligations for HMIS and for oversight of compliance with HMIS requirements.

j. To third parties for the following purposes:

i. To permit other systems of care to conduct data matches (i.e., to determine if you are also utilizing services from such other systems of care); and

ii. To permit third party research firms and/or evaluators to perform research and evaluation services in connection with the programs administered by the CCoC and the other agencies;

A. Provided that before PII is disclosed under this subsection, the third party that will receive such PII and use it as permitted above must first execute a Data Use & Disclosure Agreement requiring such third party to comply with all applicable laws and regulations, including the privacy standards and disclosure provisions contained in the Department of Housing and Urban Development Homeless Management Information Systems; Data and Technical Standards Final Notice (see 69 Federal Register 45888 (July 30, 2004)), which such standards and provisions are reflected herein.

2. Before we make any use or disclosure of your PII that is not described here, we seek your consent first.

<u>How to Inspect and Correct PII</u>.

1. You may inspect and have a copy of your PII that we maintain. We will offer to explain any information that you may not understand.
2. We will consider a request from you for correction of inaccurate or incomplete PII that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and to supplement it with additional information.
3. We may deny your request for inspection or copying of PII if:
    a. The information was compiled in reasonable anticipation of litigation or comparable proceedings;
    b. The information is about another individual (other than a health care provider or homeless provider);
    c. The information was obtained under a promise of confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information; or
    d. Disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

4. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the PII that we maintain, documentation of the request and the reason for the denial.
5. We may reject repeated or harassing requests for access to or correction of PII.

Data Retention.

1. We collect only PII that is relevant to the purposes for which we plan to use it. To the extent necessary for those purposes, we seek to maintain only PII that is accurate, complete and timely.
2. We will dispose of PII not in current use seven years after the information was created or last changed. As an alternative to disposal, we may choose to remove identifiers from the PII.
3. We may keep information for a longer period if required to do so by an applicable statute, regulation, contract or other requirement.

Complaints and Accountability.

1. We accept and consider questions or complaints about our privacy and security policies and practices. You may ask <name an individual or provide a point of contact and describe a process for submitting questions or complaints.>
2. All members of our staff (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy policy. Each staff member must receive and acknowledge receipt of a copy of this privacy policy.
3. In the event that your question or complaint is not sufficiently addressed through this organization, you may take your concerns to the Grievance Committee of the CCoC. Individuals will submit grievances in writing to the co-chairs. The co-chairs will pass the grievance to the Grievance Committee, which will review it and make a recommendation back to the co-chairs. The co-chairs will make the final decision about the outcome and notify you. More information about this Committee can be found at www.nychomeless.com. Additionally you may take your concerns to the NYC Commission on Human Rights.

NYC CCOC Coalition on the Continuum Of Care

__Appendix I__: NYC HMIS Data Standards

Appendix I is provided as a reference for contributing HMIS organizations and those considering HMIS participation.

Participation in the HMIS requires that you collect all the universal and program-specific data elements on all clients served in your program consistent with the most recent HUD HMIS Data Standards and the requirements of your program funding**.**

HUD's data standards specify the information that must be collected for each project and client, the allowable responses, the frequency with which the information must be updated, and the format in which it can be transferred across data systems, including to the NYC HMIS Data warehouse. HUD's HMIS data standards require that "*An HMIS software must be able to collect all of the data elements defined within this HMIS Data Dictionary, support the system logic, including dependencies, identified in this document, and ensure that the data collection and the visibility of data elements is appropriate to the project type and federal funding sources for any given project*" (HMIS Data Standards Data Dictionary, v. 1.3, p. 2).

The complete HMIS data standards consist of three documents:

- HMIS Data Standards Manual (https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf)
- HMIS Data Standards Data Dictionary (https://www.hudexchange.info/resources/documents/HMIS-Data-Dictionary.pdf)
- HMIS CSV Format Specifications (https://hudhdx.info/Resources/Vendors/5_1_2/HMISCSVSpecifications6_12.pdf)

These materials can be accessed at the following websites:

- https://www.hudexchange.info/resource/3824/hmis-data-dictionary/
- www.NYCHOMELESS.gov

HMIS data is used for project-level performance reporting to HUD, the NYC CCoC evaluation process, and New York City homeless assistance system reporting to HUD.

NYC CCOC Coalition on the Continuum Of Care

Appendix J: Sample Security Incident Reporting Form

CHO's must have an agency security incident reporting form to be used in the event of a security incident. At a minimum, it must include the information below. In the event of a security incident, the CHO must report it to the DSS Security Officer & HMIS lead system admin (include names & contacts).

Introduction

On [insert date MM/DD/YYYY], [insert Agency Name] experienced a security incident involving elements of our information technology infrastructure.

Provide a brief, high-level overview of the incident that occurred, what network components were affected, what the expected cause was, what measures were taken, and what the next steps will be. Limited this introduction to a single paragraph.

This report will document the security incident's following details:

- Times, dates, and activities attempted by the Information Technology (IT) department throughout the incident.
- Activities accomplished by the IT department.
- Impact of the incident on IT services and infrastructure.
- Alerting and detection methods used.
- IT's response to the incident.
- Changes made and/or required by IT as a result of lessons learned from the incident.

Timeline and Activities

Use the following table to list information from security log files. Use only those log files that pertain to the incident itself, and include any physical actions taken by IT. Attach all copies of pertinent log files to this report. How many entries are included depends on the length and type of security incident.

Date	Time	Source IP	Target	Protocol	Details

Activities Performed During Incident

Discuss here the historical context of the incident. Include any information derived from the user(s) of the system(s) or device(s) that were compromised.

Example:

- A user may have been traveling for business purposes and using his or her company laptop to log onto the Internet via Wi-Fi connections at several different airports. This would mean that the laptop was connecting without the benefit of the corporate firewall or of updated anti-virus definitions.

- Include what type of worm or Trojan IT believes infected the laptop and how IT has reached this conclusion.

Impact on IT Services

Provide full details on how the security incident impacted IT operations and services, if at all. State if the impact was high, medium, or low, based on the different services, procedures, and devices compromised. In the case of an infected laptop, operational impact on enterprise IT infrastructure would be minimal if the laptop's infection was caught early enough. From a procedural standpoint, however, the impact would be much higher.

Alerting and Detection Methods

State how or by what procedure the security incident was discovered. For instance, the laptop's infection was discovered during a normal review of firewall logs by the network administrator, or via an Intrusion Detection System.

IT's Response to Incident

1. State how long it took for IT to report the incident to senior management.

2. State how long it took to mitigate the security incident. This timeline should span the moment in which the incident was detected until the immediate threat was ended.

Next Steps and Changes Made to Prevent and Solve in the Future

Give a high-level strategic outlook of how IT security must change in order to prevent future threats from occurring. For example, "The IT security perimeter must be altered to prevent unauthorized traffic from leaving the network, such as a Trojan notifying its creator that a back door has been established. This will be enforced by updating egress rules on the corporate firewall."

- "Text":

  - "activity"

- Add any other mitigation techniques to be employed by IT.

Current Status of Incident

Updates

____

Name of person completing form   Date

Title, email, phone, main agency #

____

Executing Officer (Signature)   Date
Name, title, etc..