CCHMIS
Administration Manual

Policies and operations of the CARES of NY, Inc. Collaborative Homeless Management Information System (CCHMIS).

Version 1.2
Effective: October 1, 2022

CARES of NY, Inc.
200 Henry Johnson Blvd., Suite 4
Albany, New York 12210
(518) 431 - 4130

CARES
OF NY, INC
ENDING HOMELESSNESS

ARTICLE 1. CONTENTS

SECTION 1.1 VERSION INFORMATION

1.1.1 CURRENT VERSION

CARES OF NY, INC. COLLABORATIVE HOMELESS MANAGEMENT INFORMATION SYSTEM (CCHMIS) ADMINISTRATION MANUAL

Authored By: CARES of NY, Inc.

Date Published: 10/01/2019

Total # of Pages: 80

Version #: 1.3

Date Approved: 10/01/2022

Approved By: Kelli Clark, Assistant Director of HMIS Program and Services

Date Effective: 10/1/2020

1.1.2 REVIEW HISTORY

Date Last Reviewed: 10/01/2022

Reviewed By: Kelli Clark,

Date Due for Review: October 2023

1.1.3 REVISION HISTORY

REVISION NUMBER	REVISION DATE	REVISION BY	DESCRIPTION OF CHANGE
1.0	10/01/2019	Allyson Thiessen and Emily Rebehn	Reformatting and Update
1.1	7/1/2020	Allyson Thiessen	Update and Project name change
1.2	10/1/2020	Allyson Thiessen	Update
1.3	10/1/2022	Kelli Clark	Update

ARTICLE 2. INTRODUCTION

SECTION 2.1 DOCUMENT DESCRIPTION

2.1.1 EXECUTIVE SUMMARY

CARES of NY, Inc. (CARES) has developed the following Policies and Procedures Manual (hereafter referred to as "this document") to serve as a reference regarding the administration of the CARES Collaborative Homeless Management Information System.

This document defines the goals and objectives of the CARES Collaborative HMIS (CCHMIS) program, provides the roles and responsibilities of those involved in the program, and establishes policies and procedures for the operation of the CCHMIS. This includes CCHMIS administration, communication, security, privacy, and data quality.

2.1.2 OBJECTIVES

» Provide guidance for proper and improper use of the CCHMIS and data;

» Describe security and privacy plans to protect data confidentiality; and

» Demonstrate compliance with federal regulations.

2.1.3 TARGET AUDIENCE

The HMIS Lead, Users, CHOs, external collaborative parties, and any organizations interested in the operations of the CCHMIS.

2.1.4 DOCUMENT STRUCTURE

Information is presented within this document as follows:

Purpose	The reason for the policy/policies.
Scope	The processes to which the policy/policies apply.
Applicability	The individuals and/or entities to which the policy/policies apply.

Policy	The goal and/or expectations that are intended to guide decision-making.
Standards	Requirements to ensure a basic level of compliance and uniformity.
Procedures	The instructions to complete a process that is important to, or referenced by, a policy or standard.
Exemptions	Situations wherein the policy may not apply (where it otherwise would).
Additional Information	Guidance, suggestions, useful information, and related policies.

2.1.5 INQUIRIES

Contact the CCHMIS via email at hmis@caresny.org or by phone at (518) 489-4130 for information about the CCHMIS or the policies and procedures contained in this document, or if you are interested in joining the CCHMIS.

SECTION 2.2 BACKGROUND

2.2.1 PURPOSE OF THE HMIS

> *"The purpose of a homeless management information system (HMIS), whether funded by public or private resources, is to record and store client-level information about the numbers, characteristics, and needs of persons who use homeless housing and supportive services and for persons, who receive assistance for persons at risk of homelessness."*[1]

HMIS Proposed Rule of 2011

2.2.2 HISTORY

In 2001, the United States Congress directed the U.S. Department of Housing and Urban Development (HUD) to provide an annual report on the status of homelessness across the country[2]. To meet this demand, HUD put forth the Homeless Management Information Systems (HMIS): Data and Technical Standards Final Notice, effective August 30, 2004, for a computerized data collection system or Homeless Management Information System (HMIS) that records the characteristics, demographic information, and number of persons using homeless services across over time and location.

As per this Notice, "the development of a local HMIS is about:

> *(1) Bringing the power of computer technology to the day-to-day operations of individual homeless assistance providers;*
>
> *(2) knitting together providers within a local community in a more coordinated and effective housing and service delivery system for the benefit of homeless clients; and*
>
> *(3) obtaining and reporting critical aggregate information about the characteristics and needs of homeless persons. An HMIS provides significant opportunities to improve access to, and delivery of, housing and services for people experiencing homelessness. An HMIS can accurately describe the scope of homelessness and the effectiveness of efforts to ameliorate it. An HMIS can strengthen community planning and resource allocation.*

HUD put forth further guidance in The HMIS Proposed Rule of 2011 (24 CFR Parts 91, 576, 580, and 583- the Homeless Management Information Systems Requirements), and currently maintains the HMIS Data Standards and HMIS Data Dictionary to provide a standard method for recording information in the HMIS.

As a result, the HMIS provides a common language for discussion about the quantity and quality of services, and a basis for evaluation at the community, state, and federal levels to be used for allocation of funding and the improvement of community planning.

2.2.3 PARTICIPATION REQUIREMENTS

As per HUD regulations, all recipients of HUD McKinney-Vento Act program funds are expected to participate in an HMIS. This includes all recipients and subrecipients of the Continuum of Care (CoC) Program and Emergency Solutions Grant (ESG) funds. H that receive HOPWA funding and target homeless persons are also required to participate in HMIS.

In addition, HUD works with the U.S. Department of Health and Human Services (HHS) and the U.S. Department of Veteran's Affairs (VA) for these Federal Partner's participation in the HMIS.

See Federal Partner resources for further detailed information on programs required to participate in HMIS.

[1] As stated within Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH): Proposed Rule for HMIS Requirements, (published December 9, 2011).

[2] Discussed within Homeless Management Information Systems (HMIS): Data and Technical Standards Final Notice, effective August 30, 2004: 1.2.1. Direction to HUD on Homeless Management Information Systems.

2.2.4 THE CARES COLLABORATIVE HMIS

CARES of NY, Inc. (CARES) is a not-for-profit organization with a mission to collaborate with and support local communities towards the creation of systems to end, and prevent future, homelessness. CARES is the HMIS Lead for the CARES Collaborative HMIS (CCHMIS), a multi-Continuum HMIS that serves communities across central and upstate New York State.

To fulfill the requirements of the Continuum of Care Program (CFR Title 24 Part 578) as updated and published April 1, 2017, CARES uses the Affordable Wider Area Regional Database System (AWARDS) software from vendor Foothold Technology. Foothold Technology, as the HMIS Vendor, maintains the database in compliance with HUD specifications to preserve the integrity, security, and privacy of the data within the CCHMIS.

ARTICLE 3. GENERAL PROVISIONS

Purpose: General information that pertains to the entirety of this document, including all Plans and Appendices.

SECTION 3.1 GUIDING REGULATIONS

Purpose: To provide, generally, the rules and regulations this document is intended to ensure compliance with.
Scope: General.
Applicability: General.

3.1.1 REGULATIONS

These CCHMIS Operating Policies and Procedures were created to comply with all federal, state, and local government requirements and regulations as of the effective date. Care was taken to ensure compliance with federal HMIS regulations, which include the following:[3]

- » The McKinney-Vento Homeless Assistance Act as amended by The Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH) Act of 2009 (§808);
- » Homeless Emergency Assistance and Rapid Transition to Housing: Continuum of Care Program (77 FR 45421) of July 31, 2012;
- » HMIS Data and Technical Standards Final Notice (69 FR 45887) of July 30, 2004;
- » The HMIS Requirements Proposed Rule (76 FR 76917) of December 9, 2011, specifically the parts:
  - a. HMIS Technical Standards (Federal Register Vol. 76, No. 237 §580.33);
  - b. HMIS Privacy and Security Standards (Federal Register Vol. 76, No. 237 §580.35); and
  - c. HMIS Data Quality Standards (Federal Register Vol. 76, No. 237 §580.37);
- » 2022 HMIS Data Dictionary;
- » 2020 HMIS Data Standards Manual; and
- » Federal partner program manuals for HMIS.

3.1.2 COMPLIANCE WITH REGULATIONS POLICY

POLICY

All parties named within this document will be responsible for knowing and complying, where applicable, with the Guiding Regulations above, this document, and any other applicable federal, state, and local laws and regulations.

3.1.3 USER DISCLAIMER

POLICY

Although the HMIS Lead will monitor for compliance, the HMIS Lead will not be responsible for CHO violations of compliance. All CHOs will be held responsible for the compliance of their Users.

[3] More information on federal regulations can be found online at https://www.hudexchange.info/programs/hmis/.

SECTION 3.2 POLICY CONFLICTS

Purpose: To provide guidance in the event of difficulty implementing the policies and standards within this document.
Scope: General.
Applicability: General.

3.2.1 HIPAA REGULATIONS POLICY

POLICY

HMIS regulations were created with HIPAA regulation as guiding material and, in any situation where HIPAA regulations apply to HMIS data or operations, any and all HIPAA regulations will take precedence over the implementation and enforcement of this document.

STANDARDS

- » CHOs are responsible for knowing and complying with HIPAA regulations as they apply to their organization.

ADDITIONAL INFORMATION

The HMIS standards give precedence to the HIPAA privacy and security rules because: (1) The HIPAA rules are more finely attuned to the requirements of the health care system; (2) the HIPAA rules provide important privacy and security protections for protected health information; and (3) requiring a homeless service provider to comply with or reconcile two sets of rules would be an unreasonable burden.

3.2.2 IN ABSENCE OF A POLICY

POLICY

In the absence of a policy, any existing local, state, and federal rules and laws are to be followed and constitute policy.

ADDITIONAL INFORMATION

See HIPAA Precedence Policy.

3.2.3 IN CONFLICT OF A POLICY

POLICY

In the event of a conflict or discrepancy between this document and any other regulation (and holding true until the situation is resolved) HIPAA regulations will take precedence over this document for enforcement, followed by other federal regulations, then state regulations, and finally local regulations. When other privacy or security laws apply to a provider, the provider will comply with the requirements that ensure the greatest protection for the participant’s personally identifying information (PII).

STANDARDS

- » The HMIS Lead must be notified immediately of any policy conflicts, within two (2) business days of the discovery.

ADDITIONAL INFORMATION

See HIPAA Precedence Policy, HMIS Privacy Compliance.

3.2.4 SEVERABILITY OF POLICY

POLICY

Should any policy within this document be unenforceable or incorrect, that policy will be void and all other policies will remain in full effect.

SECTION 3.3 RELEVANT TERMINOLOGY

3.3.1 HMIS DEFINITIONS FROM HUD

From the HMIS Proposed Rule (2011)[4], the following are important terms used throughout this document:

- » **Act** means the McKinney-Vento Homeless Assistance Act, and, unless otherwise specified, as amended by the Homeless Emergency Assistance and Rapid Transition to Housing Act of 2009 (Division B of Pub. L. 111-22 (HEARTH Act) (42 U.S.C. 11371 et seq.).
- » **Continuum of Care (Continuum)** means the group composed of representatives from 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 veterans, and homeless and formerly homeless persons organized to carry out the responsibilities of a Continuum of Care established under 24 CFR part 578.
  a. **"CoC"** is used when *not* referring to the group of people responsible for the operation of the CoC; i.e., CoC is used when referring to the funding source of HUD: Continuum of Care "**CoC-funded**" or when referring to the geographic coverage area of the CoC.
  b. The term Continuum of Care or CoC is used throughout the remainder of this notice to refer to the parties that are typically responsible for developing and managing the local HMIS[5]
  c. · Continuum project refers to a distinct unit of an organization, which may or may not be funded by HUD or the Federal Partners, whose primary purpose is to provide services and/or lodging for the homeless and is identified by the Continuum as part of its service system. For example, a project funded by the HUD's CoC Program may be referred to then as a "CoC Program-funded continuum project."
  d. • CoC Program refers to the HUD funding source which provides housing and/or service grant dollars.
- » **Comparable database** means a database that is not the Continuum's official HMIS, but an alternative system that victim service providers and legal services providers may use to collect client-level data over time and to generate unduplicated aggregate reports based on the data, and that complies with the requirements of this part. Information entered into a comparable database must not be entered directly into or provided to an HMIS.
- » **Contributing HMIS Organization (or CHO)** means an organization (including its employees, volunteers, affiliates, contractors, and associates) that operates a project that contributes Protected Identifying Information (PII) on homeless clients to an HMIS.
- » **Data recipient** means a person who obtains personally identifying information from an HMIS Lead or from a CHO for research or other purposes not directly related to the operation of the HMIS, Continuum of Care, HMIS Lead, or CHO.
- » **Homeless Management Information System (HMIS)** means the information system designated by Continuums of Care to comply with the requirements of this part and used to record, analyze, and transmit client and activity data in regard to the provision of shelter, housing, and services to individuals and families who are homeless or at risk of homelessness.
- » **HMIS Lead** means an entity designated by the Continuum of Care in accordance with this part to operate the Continuum's HMIS on its behalf.
- » **HMIS Vendor** means a contractor who provides materials or services for the operation of an HMIS. An HMIS vendor includes an HMIS software provider, web server host, data warehouse provider, as well as a provider of other information technology or support.

[4] HMIS Requirements Proposed Rule 2011

[5] 2004 HMIS

- **HUD** means the Department of Housing and Urban Development.
- **Participation fee** means a fee the HMIS Lead charges CHOs for participating in the HMIS to cover the HMIS Lead's actual expenditures, without profit to the HMIS Lead, for software licenses, software annual support, training, data entry, data analysis, reporting, hardware, connectivity, and operating the HMIS.
- **Protected identifying information (PII)** means information about a program participant that can be used to distinguish or trace a program participant's identity, either alone or when combined with other personal or identifying information, using methods reasonably likely to be used, which is linkable to the program participant.
- **Project** refers to specific, grant-funded projects operated by a provider and set up within the HMIS as distinct units.
- **Program** refers to a federal funding source.
- **Unduplicated count of homeless persons** means an enumeration of homeless persons where each person is counted only once during a defined period.
- **User** means an individual who uses or enters data in an HMIS or another administrative database from which data is periodically provided to an HMIS.
- **Victim service provider** means a private nonprofit organization whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking. This term includes rape crisis centers, battered women's shelters, domestic violence transitional housing programs, and other programs.

HMIS Data Standards Terms and Concepts

Continuum of Care (CoC) is used in multiple ways throughout the Data Standards:
Continuum of Care and Continuum means the group organized to carry out the responsibilities required under the CoC Program Interim Rule (24 CFR Part 578) and comprises 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, and law enforcement, and organizations that serve homeless and formerly homeless persons to the extent that these groups are represented within the geographic area and are available to participate.

9/3/2019 5
CoC Program refers to the HUD funding source which provides housing and/or service grant dollars.

Continuum project refers to a distinct unit of an organization, which may or may not be funded by HUD or the Federal Partners, whose primary purpose is to provide services and/or lodging for the homeless and is identified by the Continuum as part of its service system. For example, a project funded by the HUD's CoC Program may be referred to then as a "CoC Program-funded continuum project."

HMIS User means the individual who uses or enters data in an HMIS or a comparable database approved by the CoC.

HMIS Lead means the entity designated by the Continuum of Care in accordance with the HMIS Proposed Rule (24 CFR Part 580) to operate the Continuum's HMIS on the Continuum's behalf. As of May 2019, the HMIS Rule is not in effect. When HUD publishes the final HMIS Rule communities will be given time to come into compliance with the rule.

HMIS System Administrator means the individual(s) whose job it is to manage the HMIS implementation at the local level: enrolling programs and managing appropriate use, supporting users through connection to, or direct provision of, user training, and overseeing system setup.

Project and Program are terms used to mean different things across the federal agencies. In this document, and for the purposes of data collection in HMIS, a ***program*** refers to the federal funding source (e.g., HUD CoC, HHS PATH, VA SSVF, etc.) whereas ***project*** refers to a distinct unit of an organization as set up in the HMIS.

3.3.2 ADDITIONAL HMIS TERMINOLOGY

- **Vendor CHO** means a CHO that contracts for HMIS services with the Continuum's chosen HMIS software vendor directly through an independent contract.
- **Incident** means an event that may indicate that the security of an organization's systems or data has been compromised, or that measures put in place for protection have failed. (Example: A device is stolen that contains HMIS data.)
- **Data owner/ownership** means, in general, a data owner is a person or organization with the legal right and ability to create, alter, share, or restrict any piece or set of data. Data owners can assign these functions and responsibilities to other parties (e.g., a system provider) to act on their behalf. These providers host data systems to store and process the data and often have the same capabilities as the owner to edit, share, or restrict data.
- **Disaster** means either man-made (e.g., theft, equipment failure) or natural (weather) event that results in an interruption of service or have the possibility to compromise data.
- **HIPAA** means the Health Insurance Portability and Accountability Act of 1996, United States legislation that provides data privacy and security provisions for safeguarding medical information.
- **Technical Assistance (TA)** means assistance and guidance to facilitate the implementation and success of day-to-day operations of the HMIS, often involving the delivery of specific training programs.
- **No-show** means an User that does not properly cancel and does not attend a training they were registered to attend.

- **Privacy documents** means any written or otherwise documented agency privacy notices, statements, policies, or procedures.
- **Processing** means any operation or set of operations performed on PPI, whether or not by automated means, including but not limited to collection, maintenance, use, disclosure, transmission and destruction of the information.

ARTICLE 4. ROLES & RESPONSIBILITIES

Purpose: To provide expectations of and designate the role, responsibilities, and duties of the parties responsible for, or to, the HMIS and/or HMIS data.

SECTION 4.1 GUIDING PRINCIPLES

Scope: General.
Applicability: General.

4.1.1 CODE OF ETHICS

POLICY

The following rules govern the actions of all individuals involved with, responsible for, or responsible to the HMIS, and these rules are assumed to be included and hold true within all other policies:

1. HMIS data will be used towards the improvement of homeless services.
2. HMIS data will be protected to the highest degree, and only used by authorized parties for authorized purposes.
3. Users will strive to provide the highest quality data possible.
4. The rights of all HMIS clients, as provided for within this document and the CCHMIS Privacy Notice, will be respected.

4.1.2 ROLE AND RESPONSIBILITY POLICY

POLICY

Each entity will be held responsible for their enumerated responsibilities and for abiding by the Code of Ethics.

SECTION 4.2 MANAGEMENT & OVERSIGHT

Scope: HMIS management and administration.
Applicability: The Continuum of Care.

4.2.1 CONTINUUM OF CARE

ROLE

The Continuum of Care is responsible for making decisions about HMIS management and administration and is responsible for ensuring that its HMIS is operated in accordance with all applicable federal, state, and local laws and regulations.

RESPONSIBILITIES

The Continuum must:

- Designate a single information system as the official Homeless Management Information System (HMIS) software for the geographic area, and ensure the software meets all HUD HMIS requirements;
- Designate an eligible applicant (be a state or local government, an instrumentality of state or local government, or a private nonprofit organization) to manage the Continuum's HMIS, which will be known as the HMIS Lead;
- Ensure consistent participation in the HMIS by recipients of funds from the Emergency Solutions Grants Program and from the other programs authorized by Title IV of the McKinney-Vento Act across the geographic area of the Continuum;
- Work with the HMIS Lead to:

a. Ensure the HMIS is operated in compliance with requirements prescribed by HUD.
    i. Ensure the HMIS software can report unduplicated data for each Continuum of Care to support the multi-Continuum HMIS configuration.
    ii. Ensure that HMIS processing capabilities remain consistent with the privacy obligations of the CHO;

b. Develop and maintain an HMIS governance charter;

c. Ensure each CHO enters into a CCHMIS CHO Agreement (participation and confidentiality agreement);

d. Ensure CHOs meet or exceed data quality requirements;

e. Review, revise, and approve the policies and plans developed by the HMIS Lead for the HMIS as necessary or required by HUD and ensure these plans include a privacy plan, a security plan, and a data quality plan;

» Maintain documentation evidencing compliance with the governance charter; and

» Be responsible for ensuring HMIS data is collected to a centralized location at least once a year from all Users within the Continuum;

» Approve any additional data elements for HMIS collection and entry for specific programs within the Continuum or for the Continuum as a whole; and

» Be responsible for imposing sanctions on CHOs for failure to comply with any HMIS requirements, as per applicable federal rules.

ADDITIONAL INFORMATION

HMIS Lead Designation MOU Policy.

4.2.2 DATA COMMITTEE

ROLE

A Data Committee will convene within each Continuum of Care on a regular basis to discuss the Continuum's data and report information back to the Continuum's projects and the community.

RESPONSIBILITIES

The Data Committee must:

» Be organized and overseen locally within each Continuum;

» Review aggregate HMIS data on the demographics of consumers within the Continuum;

» Assist in identifying weaknesses and trends in HMIS data, and work closely with the HMIS Lead on data-related issues;

» Review and report on data to the Continuum and community regularly; and

» Provide data-based guidance to the Continuum.

STANDARDS

» Every Data Committee must have a chair, or two co-chairs, and at least 3 other members.

SECTION 4.3 GOVERNANCE

Scope: Oversight of the CCHMIS.
Applicability: CCHMIS Advisory and Implementation Committees.

PLEASE NOTE*: The information provided within this section refers to the CCHMIS Governance Charter; please see the HMIS Governance Charter Policy and the CARES Collaborative HMIS Governance Charter for more information.*

4.3.1 CCHMIS ADVISORY COMMITTEE

ROLE

A part of the CCHMIS governance structure, the CCHMIS Advisory Committee will provide ongoing supervision to, and guide the actions of, the HMIS Lead.

RESPONSIBILITIES

The CCHMIS Advisory Committee must:

- Convene regularly to evaluate the HMIS and ensure it meets HUD requirements;
- Report to communities on policies regarding: consumer privacy and confidentiality, reporting schedules, information sharing, software choices, and monitoring; and
- Dictate the activation and deactivation of the CCHMIS Implementation Committee, as necessary.

STANDARDS

- Two (2) representatives are nominated and approved within each Continuum for the HMIS Advisory Committee following the Continuum's Committee Nomination and Selection process.
- One (1) representative per CHO is allowed, unless a majority of representatives agree to waive this restriction for a small Continuum to respect the need for knowledgeable and capable persons on committees.
- Chairs/Co-chairs of a Continuum are not eligible for membership on the CCHMIS Advisory Committee.

PROCEDURES

MEETINGS

1. The CCHMIS Advisory Committee meets the 4th Wednesday of each month at 10am, unless otherwise specified.

CONTACT

2. You may contact your advisory committee representative with programmatic HMIS concerns that you would like to have addressed during the next meeting. A list of CCHMIS Advisory Committee members with contact information is posted on the HMIS Lead website: https://caresny.org/ .
3. For information on the committee, the process, or the log-on for the next webinar, contact the Director of HMIS Programs and Services: https://caresny.org/cchmis/#Our-Team.

4.3.2 CCHMIS IMPLEMENTATION COMMITTEE

ROLE

A part of the CCHMIS governance structure , the CCHMIS Implementation Committee is a non-essential, temporary entity that will, on behalf of a Continuum, facilitate the implementation of the CCHMIS in a new community.

RESPONSIBILITIES

The Implementation Committee must:

- Be activated and deactivated at the discretion of the CCHMIS Advisory Committee;
- Convene regularly during active periods to support the HMIS Lead with research, evaluation, and negotiation of a contract with the HMIS vendor;
- Assist in obtaining community support and coordinating the implementation of HMIS across the Continuum; and
- Establish initial community goals for the HMIS.

STANDARDS

- At least one (1) representative must be a member of the new community.
- At least one (1) representative must be a member of the CCHMIS Advisory Committee.

SECTION 4.4 ADMINISTRATION

Scope: HMIS Lead administration of the CCHMIS.
Applicability: HMIS Lead.

4.4.1 HMIS LEAD

ROLE

The HMIS Lead is designated by the Continuum of Care and will be responsible for facilitating the success of the HMIS for all participating organizations within a Continuum, including implementing and administrating the HMIS; conducting oversight of the HMIS; and taking corrective action, if needed, to ensure that the HMIS is compliant with all federal HMIS requirements.

RESPONSIBILITIES

The HMIS Lead must:

- Provide system administration and operation:
    a. Sign a contract with an HMIS vendor for HMIS database software and services and ensure that this contract requires the HMIS Vendor to provide meet HUD and other federal regulations and standards (see Contracts section for details);
    b. Handle the billing and payments for the HMIS software;
    c. Execute a written CCHMIS CHO Agreement (participation and confidentiality agreement) with each CHO which includes the obligations and authority of the HMIS Lead and CHO, and an agreement that the HMIS Lead and the CHO will process Protected Identifying Information consistent with the agreement;
    d. Maintain a level of staffing to fulfill the requirements of the HMIS Lead in all contracts and agreements;
    e. Provide HMIS-related services via Technical Assistance contracts;
- Provide HMIS training:
    a. Provide ongoing training, technical assistance, database management, and reporting support to the CHOs;
    b. Provide Help desk operation and end User support for the HMIS;
- Engage in governance, management, and collaboration with the Continuum to:
    a. Ensure participation by recipients of funds from the Emergency Solutions Grants Program and from the other programs authorized by Title IV of the McKinney-Vento Act;
    b. Ensure the HMIS software can report unduplicated data for each Continuum of Care to support the multi-Continuum HMIS configuration.
    c. Submit reports to HUD as required;
    d. Serve as the applicant to HUD for grant funds to be used for HMIS activities for the Continuum of Care's geographic area, as directed by the Continuum, and, if selected for an award by HUD, enter into a grant agreement with HUD to carry out the HUD-approved activities;
- Engage in policy development and implementation:
    a. Develop written policies and procedures for the operation of the HMIS that apply to the HMIS Lead, its CHOs, and the Continuum of Care, and ensure that these comply with all applicable federal law and regulations, and applicable state or local governmental requirement;
    b. Develop and maintain written plans (Privacy, Security, Data Quality);
- Provide monitoring and oversight for the HMIS:
    a. Develop data quality benchmarks;
    b. Monitor and enforce compliance of all CHOs with HMIS requirements and report on compliance to the Continuum;

- Engage in data analysis/reporting on the HMIS:
  a. Provide data to CHOs to monitor data quality;
  b. Assist CHOs with data analysis for grant writing; and
  c. Provide data to Data Committees, which Data Committees use to make recommendations and provide guidance to their respective Continuums.

4.4.2 HMIS DIRECTOR

ROLE

The HMIS Director will guide the HMIS Lead staff and ensure the HMIS complies with Federal HMIS regulations, support CHOs in required reporting, and ensure HMIS grant applications adequately provide for successful HMIS Lead function.

RESPONSIBILITIES

The HMIS Director must:

- Ensure all HMIS Lead responsibilities are fulfilled;
- Maintain current knowledge of HUD requirements;
- Ensure compliance of the HMIS with current federal regulations;
- Develop community relationships and encourage participation from non-required programs;
- Submit reports to HUD as required;
- Provide support to all HMIS Lead staff; and
- Attend regional and national conferences to keep current with industry best practices.

4.4.3 HMIS SYSTEM ADMINISTRATOR

ROLE

The HMIS Lead System Administrator will be dedicated to administrating and maintaining the HMIS database to ensure the success of all CHOs.

RESPONSIBILITIES

The HMIS System Administrator must:

- Communicate with the system vendor on system problems;
- Have regular contact with HUD technical assistance CHOs.
- Customize the HMIS as necessary;
- Support CHOs with reporting requirements;
- Attend and participate in local Continuum, Data Committee, and any other HMIS-related meetings as necessary;
- Help ensure data quality among all CHOs;
- Track bed and unit inventory information, by project, as is relevant for federal reports and utilization analyses; and
- Ensure that all HMIS-related information pertaining to changes and updates in federal regulations is disseminated to all CHOs as necessary.

4.4.4 HMIS CUSTOMER SERVICE REPRESENTATIVE

ROLE

The HMIS Customer Service Representative will be dedicated to training and supporting Users.

RESPONSIBILITIES

The HMIS Customer Service Representative must:

- Provide local support, training, and/or technical assistance to CHOs and partnering organizations;

- » Provide on-call support to Users;
- » Manage the HMIS HelpDesk and promptly address all issues that arise with Users; and
- » Assist the System Administrator in customizing or altering the HMIS as necessary.

4.4.5 HMIS DATA ANALYST

ROLE

The HMIS Data Analyst will be dedicated to the technical maintenance of the database, data analysis, and reporting.

RESPONSIBILITIES

The HMIS Data Analyst must:

- » Provide reports to the community and planning parties regarding HMIS data;
- » Assist the HMIS Data Quality Associate in monitoring CHO data quality; and
- » Assist in the upload of new information to the HMIS.

4.4.6 HMIS QUALITY ASSURANCE ASSOCIATE

ROLE

The HMIS Quality Assurance Associate will be dedicated to improving the quality of HMIS data.

RESPONSIBILITIES

The HMIS Data Quality Associate must:

- » Monitor CHOs for data quality;
- » Work with CHOs to improve data quality; and
- » Assist uploading CHOs to improve data quality.

4.4.7 HMIS SECURITY OFFICER

ROLE

The HMIS Security Officer will be dedicated to the security of the HMIS database to maintain the confidentiality of HMIS data.

RESPONSIBILITIES

The HMIS Security Officer must:

- » Update and maintain the security of HMIS Lead operations to meet or exceed HUD and industry standards, including internal infrastructure and physical workspace as per industry best practices;
- » Address any security issues that arise;
- » Routinely evaluate the HMIS Lead for security risks and correct risks in a timely fashion; and
- » Review and assist in updating security requirements as necessary.

SECTION 4.5 CONTRIBUTING ORGANIZATIONS

Scope: CHO actions.
Applicability: CHOs.

4.5.1 CONTRIBUTING HOMELESS ORGANIZATION

ROLE

A Contributing Homeless Organization (or “CHO”) in the Continuum will enter into a contract for HMIS services with the Continuum’s chosen HMIS software vendor (through the HMIS Lead or directly through an independent contract with the HMIS vendor) and will enter data into the HMIS as required, including – to the best of their ability – meeting any completeness, quality, and timeliness requirements. A CHO will also be responsible for the compliance of their staff with respect to maintaining the confidentiality of client-level HMIS data and will ensure compliance with all State and Federal regulations, including HIPAA requirements, as they apply to their organization.

RESPONSIBILITIES

A CHO must:

- Enter a contract for HMIS services with the Continuum's chosen HMIS software vendor:
    a. Through a contract with the HMIS Lead; or
    b. Directly with the HMIS vendor through an independent contract.
        i. These organizations are referred to as Vendor CHOs within this document.

PLEASE NOTE*: Vendor CHOs will not receive all HMIS services from the HMIS Lead, but* ***are*** *required to follow all policies for CHOs as described within this document unless specifically exempted within the policy;*

- Enter into a CCHMIS CHO Agreement with the HMIS Lead that will outline the requirements of the CHO and the HMIS Lead to ensure a successful HMIS implementation, which will include that the CHO will:
    a. Be held responsible for any misuse of the HMIS by its Users.
    b. Designate a staff member to be the Agency HMIS Administrator and HMIS Security Officer for the CHO;
    c. Comply with all privacy and security requirements outlined in this document, as well as requirements in the CHO HMIS Agreement;
    d. Comply with Federal, state, and local laws that require additional privacy or confidentiality protections; and
    e. Implement procedures to ensure and monitor its compliance with applicable agreements and HUD requirements, including enforcement of sanctions for noncompliance, as an organization with access to protected identifying information, including:
        i. Monitoring for and enforcing staff compliance in all activities associated with User access of the HMIS.

4.5.2 CHO ADMINISTRATOR

ROLE

The Agency HMIS Administrator will receive additional HMIS training and will be responsible for the data quality, security, and privacy of the CHO's use of the HMIS.

RESPONSIBILITIES

The Agency HMIS Administrator must:

- Ensure the CHO is in compliance with privacy and security requirements per the security and privacy policies of the HMIS;
- Maintain a CHO User roster, and submit a HelpDesk ticket when changes need to be made;
- Assist Users with problems and serve as an initial HelpDesk resource for Users at the CHO;
- Monitor data quality at least once a month;
- Work with the HMIS System Administrator as necessary on data quality issues;
- Ensure that all critical and necessary HMIS information is disseminated to all Provides and Users (e.g. changes in data collection or data entry standards, or security updates);
- Prepare for HMIS audits;
- Complete annual Privacy training; and
- Serve as the HMIS Security Officer for the CHO.

SECTION 4.6 USERS

Scope: User actions.
Applicability: Users.

4.6.1 USERS

ROLE

Users are persons who access the HMIS with User accounts to perform job duties.

RESPONSIBILITIES

An User must:

» Enter into the CCHMIS User Agreement and abide by all its requirements, including:

   a. HMIS Data collection requirements;
   b. HMIS Data entry requirements;
   c. HMIS use requirements; and
   d. Maintenance of client confidentiality.

» Maintain compliance with all required trainings and documentation.

ARTICLE 5. CONTRACTS & AGREEMENTS

Purpose: To provide for the required documentation for the administration of the HMIS, and to ensure that all contracts and arrangements executed as part of the HMIS administration are executed and maintained in compliance with all federal requirements.

SECTION 5.1 HMIS ARRANGEMENTS

Scope: The documents necessary for the administration of the HMIS within a Continuum of Care.
Applicability: The CoC, HMIS Lead.

5.1.1 COC HMIS DESIGNATION MEMORANDUM OF UNDERSTANDING (MOU) POLICY

POLICY

A participating CoC and the HMIS Lead will sign an HMIS Lead Memorandum of Understanding where the CoC designates the HMIS Vendor/software and the HMIS Lead for the Continuum, allowing the HMIS Lead to have access to the Continuum's data for the purposes of HMIS administration. This HMIS Lead Designation MOU will detail the responsibilities of the Continuum, the HMIS Lead, and CHOs as it pertains to the operation of the HMIS, as well as how the HMIS will be funded As the CCHMIS is a multi-Continuum HMIS, this MOU will include provisions to meet the requirements for a multi-Continuum HMIS as per the 2011 HMIS Proposed Rule Subpart B – HMS Administration § 580.5.[6]

STANDARDS

- » An HMIS Lead Designation MOU must be signed by the HMIS Program Director for the HMIS Lead.
- » An HMIS Lead Designation MOU must be signed by an authorized member of the Continuum on behalf of the CoC.
- » An HMIS Lead Designation MOU must be completed every year as part of the CoC Grant Application.
- » At a minimum, an HMIS Lead Designation MOU must specify:
  - a. The scope of work;
  - b. The term limit for the project;
  - c. The goals of the project;
  - d. The benefit to the homeless community;
  - e. The HMIS participation requirements;
  - f. The parties involved;
  - g. The responsibilities of each party; and
  - h. How the HMIS will be funded.

PROCEDURES

MULTI-CONTINUUM HMIS

1. As the CCHMIS is a multi-Continuum HMIS, all Continuums of Care that participate in the CCHMIS have the following specified within their HMIS Lead Designation MOU:
   a. The Continuum of Care designates Foothold Technology's AWARDS system the official HMIS software, the CCHMIS as the official HMIS for the Continuum, and CARES of NY, Inc. as the official HMIS Lead for the Continuum; and
   b. The Continuum of Care adopts the CCHMIS governance, technical, security, privacy, and data quality standards for the operation of their HMIS.

[6] HMIS 2011

ADDITIONAL INFORMATION

A template HMIS Lead Designation MOU is available from the HMIS Lead Program Director.

See Research MOU Policy for details regarding Research MOUs.

5.1.2 HMIS GOVERNANCE CHARTER POLICY

POLICY

As a multi-Continuum HMIS, the CCHMIS will have a single, joint HMIS Governance Charter that applies to the HMIS Lead and all Continuums of Care that choose to participate in the CCHMIS. The HMIS Lead will develop and maintain, with review and approval by all participating Continuums, this joint CCHMIS Governance Charter.

STANDARDS

» At minimum, the CCHMIS Governance Charter must include:

a. A requirement that the Continuum and the HMIS Lead enter into a formal agreement (Memorandum of Understanding) representative of the HMIS Lead designation that outlines management processes, responsibilities, decision-making structures, and oversight of the HMIS project;

b. A requirement that the HMIS Lead enter into written HMIS Participation Agreements with each CHO requiring the CHO to comply with all privacy, security, and data quality requirements and imposing sanctions for failure to comply; and

c. Addresses fees for participation in the HMIS.

» As the CCHMIS is a multi-Continuum HMIS, the CCHMIS Governance Chart must also specify:

a. That each Continuum of Care designates the same information system as the official HMIS software; and

b. That all Continuums of Care designate the same HMIS Lead and must work jointly with the HMIS Lead to develop and adopt a joint governance charter;

c. That all Continuums of Care within a multi-continuum HMIS designate the same governance, technical, security, privacy, and data quality standards; and

d. To be a multi-Continuum HMIS, the HMIS must be capable of reporting unduplicated data for each Continuum of Care separately.

ADDITIONAL INFORMATION

View the CARES Collaborative HMIS Governance Charter.

5.1.3 HMIS PARTICIPATION POLICY

POLICY

The Continuum of Care, with the HMIS Lead, will work with all homeless service provider organizations within the geographic coverage area of the CoC to increase participation in HMIS to the benefit of the CoC. CoC-funded programs will be required to work with the HMIS Lead to participate in the HMIS, and non-CoC-funded programs required to participate in the HMIS may do so under individual HMIS service contracts with the HMIS Lead or the HMIS Vendor. Organizations with programs serving victims of abuse, neglect or domestic violence (victim service providers) will not be allowed to participate in the HMIS but will be required to provide the Continuum with data from a comparable database to meet federal reporting requirements.

STANDARDS

» CoC-funded programs must report all required client-level HMIS data at least once per year to a central data storage facility designated by the Continuum to make it possible for the Continuum to eliminate duplicate records and analyze the data for local planning purposes.

PROCEDURES

1. The HMIS Lead operates the central data storage location for a participating Continuum of Care.

ADDITIONAL INFORMATION

Participation in the HMIS by organizations that do not receive HUD or federal partner funding is voluntary. However, the Continuum is strongly recommended to encourage participation by all homeless service provider organizations to achieve an accurate picture of homelessness within the CoC, as well as to aid the CoC in the grant competition (such as achieving service coverage and bed coverage rates, as per Federal Register Vol. 76, No. 237 § 580.37 Data quality standards and management).

See Victim Service Provider Policy.

SECTION 5.2 HMIS CONTRACTS

Scope: Contracts executed as part of HMIS administration.
Applicability: The CoC, HMIS Lead, HMIS Vendor, CHOs.

5.2.1 HMIS VENDOR CONTRACT POLICY

POLICY

The HMIS Lead will enter into a contract for an HMIS system with the HMIS vendor indicated in the HMIS Lead Designation MOU for a Continuum of Care. This HMIS Vendor contract will require the HMIS Vendor to meet all HMIS requirements established by HUD in notice.

STANDARDS

» The HMIS Vendor contract must include requirements that the HMIS Vendor complies with HMIS standards issued by HUD, including but not limited to:

a. HMIS Technical Standards (Federal Register Vol. 76, No. 237 §580.33);
b. HMIS Security Standards (Federal Register Vol. 76, No. 237 §580.35);
c. Data Quality Standards (Federal Register Vol. 76, No. 237 §580.37); and
d. Current HMIS Data Standards.

PROCEDURES

HMIS VENDOR & CONTRACT FOR SERVICES

1. The CCHMIS is in contract with Foothold Technology for use of the AWARDS system for HMIS.

5.2.2 COC-FUNDED PROGRAM CONTRACT POLICY

POLICY

The HMIS Lead will provide HMIS services within participating Continuums of Care as specified within the HMIS Lead Designation MOU. In general, homeless services providers with CoC-funded programs within participating Continuums of Care will be provided services by the HMIS Lead without a separate contract for HMIS services.

Providers with CoC-funded programs within participating Continuums of Care that underfund the HMIS may be expected to enter into a paid service contract to receive HMIS services, or any providers that operate non-CoC-funded programs required to participate in HMIS may be expected to enter into a paid service contract to receive HMIS services for these programs.

STANDARDS

» All contracts must meet HUD HMIS requirements and all other applicable federal, state, and local law.

EXEMPTIONS

Exemptions to this policy may be granted at the discretion of the HMIS Program Director.

ADDITIONAL INFORMATION

Examples of non-CoC-funded programs required to participate in the HMIS include: SSVF, RHY, HOPWA, and ESG.

***Please note**: This policy is referring to a contract for services, not the CCHMIS CHO Agreement.*

5.2.3 VENDOR CHO CONTRACT POLICY

POLICY

Organizations that contract with the HMIS Vendor for HMIS services ("Vendor CHOs") will receive more limited services from the HMIS Lead.

STANDARDS

- Vendor CHOs must execute a Technical Assistance contract with the HMIS Lead to receive additional HMIS Lead services.

PROCEDURES

DATA UPLOADS

1. Vendor CHOs must upload data from their HMIS database to the HMIS Lead database at least once per month, as per the CCHMIS CHO Agreement.
   a. The HMIS Lead may assist with this process; see the Data Quality Plan.

5.2.4 TECHNICAL ASSISTANCE CONTRACT POLICY

POLICY

An organization may request HMIS-related technical assistance (TA) from the HMIS Lead, and such requests will be fulfilled at the discretion of the HMIS Program Director. Accepted requests will require a written contract between the organization operating the program and the HMIS Lead to define the services provided, the scope of work, applicable fees, and the requirements and obligations of both the organization and the HMIS Lead. No paid services will be provided by the HMIS in absence of a written contract.

STANDARDS

- Requests for TA by a specific date must be made to the HMIS with reasonable notice, defined as that which will allow for successful service provision by the HMIS within normal business day operations. The HMIS Program Director may decline a request due to inadequate notice.
- All involved parties must sign a contract prior to the start of work.
- Services must be written into the contract to be expected of and provided by the HMIS Lead.
- No paid services will be provided by the HMIS Lead in absence of a written contract.

PROCEDURES

REQUESTS FOR TECHNICAL ASSISTANCE

1. Requests for technical assistance (TA) (*Project synopsis*/request;
   a. Any relevant deadlines; and
   b. Return contact information (minimum of name and email address or phone number).
2. Table 1) must be made in writing to the HMIS Program Director and include the following:
   a. Project synopsis/request;
   b. Any relevant deadlines; and
   c. Return contact information (minimum of name and email address or phone number).

Table 1. Types of technical assistance (TA).

TITLE	DESCRIPTION	FEES
STANDARD TA FOR CHOs	Standard HMIS services provided to CHOs by the HMIS Lead as per an executed contract between the CHO and the HMIS Lead.	None
STANDARD TA FOR VENDOR CHOs	Standard HMIS services provided by the HMIS Lead to CHOs that are NOT within an executed contract between the CHO and the HMIS Lead.	Variable cost; Billed at base hourly rate (See Fees in Appendix.)

EXTENDED TA	Services that are not provided for by a CHO 's HMIS Participation Contract, generally those that are extensive in the time and resources required to facilitate success. Possible services include, but are not limited to: Basic computer instruction for HMIS use; CHO-level training on non-CoC features of the HMIS; Operational design and the HMIS; Data quality issue repair; Large HelpDesk ticket resolution; and Database customization via form- and report-building.	Variable cost; Billed at base hourly rate (See Fees in Appendix.)
PROGRAM CUSTOMIZATION/ GRANT WRITING/ HMIS INTEGRATION	Possible services include, but are not limited to: Building custom forms and reports; Assisting programs in integrating HMIS into their daily intake and reporting needs; Negotiating system changes with the software vendor; Gathering CHO-wide or county-wide aggregate information for grant applications; or Better integration of HMIS software use into existing procedures. Assistance provided via telephone, web conferences, and/or site visits.	Variable cost; Billed at base hourly rate (See Fees in Appendix.)
OUTSIDE TA	Services provided to non-CHOs by the HMIS.	Variable cost; Billed at base hourly rate (See Fees in Appendix.)
DOMESTIC VIOLENCE (DV)-DEDICATED PROGRAM TA	DV programs are prohibited from participating in the HMIS by the Violence Against Women Act (VOWA). Some funding types, however, require each CHO to have a comparable database to the HMIS for these programs. The HMIS offers a contract to transfer the burden of ensuring that the database meets HMIS regulations onto the HMIS Lead Director.	Variable cost.
DEPARTMENT OF SOCIAL SERVICES TECHNICAL ASSISTANCE	The HMIS is offering technical assistance to New York State Department of Social Services agencies to meet state reporting requirements. Assistance offered includes: Completion of reports; Data aggregation; and Back data entry. Any combination of these services may be requested; interested agencies should contact the HMIS Program Director.	Variable cost.

3. The HMIS Program Director will review the request for TA and respond.
    a. Requests within the bounds of an existing contract will not incur additional costs.
    b. Requests not within the bounds of an existing contract will be deemed a paid service and will require a contract.

FEES FOR SERVICES

4. If the request is a paid service and the HMIS Program Director accepts it:
    a. The HMIS Program Director will provide a scope of work assessment, including:
        i. The services to be provided;
        ii. Terms of work, including start and end dates; and
        iii. Projected costs.
5. The HMIS Lead Director will work with the organization to develop an acceptable service contract.
    a. The fee schedule will be decided prior to the start of work;
        i. Fixed cost or billed at an hourly rate. See Fees for costs.

6. All paid services will be written into a service contract between the requestee and the HMIS.
   a. All parties must sign the contract prior to the start of work.
7. Once the contract is completed and signed by all parties, the HMIS Lead will begin to provide services.

SECTION 5.3 HMIS AGREEMENTS

Scope: Confidentiality agreements with the HMIS Lead for HMIS system use.
Applicability: HMIS Lead, CHOs, Users.

5.3.1 HMIS LEAD PROVISION OF CONFIDENTIALITY AGREEMENTS POLICY

POLICY

The HMIS Lead will develop and maintain confidentiality agreements for CHOs and for individuals at CHOs who require access to the HMIS and HMIS PII. These Agreements will include promises to comply with CCHMIS privacy and security policies, to meet CCHMIS data quality requirements, and to generally protect and ensure the confidentiality of client data within the CCHMIS. These Agreements will also include appropriate sanctions for violation. The HMIS Lead will regularly review and update these agreements to ensure compliance with HUD regulations.

STANDARDS

» Agreements must include requirements to comply with privacy and security measure and to maintain the confidentiality of HMIS information.

» Agreements must contain promises to maintain client confidentiality, including after termination of organizational affiliation.

» Agreements must contain sanctions for violations.

» The HMIS Lead must review these agreements at least annually and update as necessary.

ADDITIONAL INFORMATION

See CCHMIS CHO Agreement Policy, CCHMIS User Agreement Policy.

5.3.2 CCHMIS CHO AGREEMENT POLICY

POLICY

Every organization participating in the CCHMIS, regardless of the entity providing their HMIS services, will execute a participation and confidentiality agreement with the HMIS Lead. By signing this Agreement, CHOs will agree to comply with CCHMIS privacy and security policies, to meet CCHMIS data quality requirements, and to generally protect and ensure the confidentiality of client data within the CCHMIS.

STANDARDS

» CHOs must renew Agreements annually.

PROCEDURES

AGREEMENTS

1. Overall, the confidentiality and participation agreement for every CHO to enter into with the CCHMIS for participation in the CCHMIS is called the "CCHMIS CHO Agreement".
   a. Generally, agreements include the following:
      i. Requirements to comply with security, privacy and data quality requirements;
      ii. Requirements to comply with HMIS monitoring;
      iii. Designation of the Agency HMIS Administrator/HMIS Security Officer;
      iv. Designation of the data sharing preferences of the projects that the CHO operates; and
      v. If a CHO has HIPAA compliance obligations.

2. The different versions of the CCHMIS CHO Agreement are listed below, with different agreements to reflect the disparate arrangements of each situation:
   a. *CCHMIS CHO Agreement – CoC Participant*: Organizations required to participate in HMIS that work with the HMIS Lead;
   b. *CCHMIS CHO Agreement – Vendor*: Organizations required to participate in HMIS that contract with the HMIS Vendor for HMIS participation;
      i. These agreements will require monthly uploads to the HMIS Lead HMIS database from the Vendor CHO HMIS database.
   c. *CCHMIS CHO Agreement – Non-Required*: Organizations not required to participate in HMIS that are in contract with the HMIS Lead for HMIS participation; and
   d. *CCHMIS CHO Agreement - Victim Service Provider*;
      i. This agreement will specify that the organization must NOT participate in the HMIS, but instead must report aggregate, non-identifying data to the Continuum (not the HMIS Lead) from a comparable database.

EXECUTION

1. CHOs sign an CCHMIS CHO Agreement with the HMIS Lead prior to joining the CCHMIS and every year thereafter to continue participation.
   a. Existence of a complete and valid CCHMIS CHO Agreement is part of the HMIS Monitoring process.

5.3.3 CCHMIS USER AGREEMENT POLICY

POLICY

Every individual will execute a CCHMIS User Agreement that promises to maintain the confidentiality of CCHMIS data to obtain User credentials to access the CCHMIS. By signing this Agreement, Users will agree to comply with the requirements prescribed within including data collection procedures, maintenance of client privacy, and compliance with CCHMIS and their own CHO's policies and procedures.

STANDARDS

» Users must renew Agreements annually.

PROCEDURES

EXECUTION

1. The HMIS Lead provides a blank copy of the CCHMIS User Agreement on its website: https://caresny.org/cchmis.
2. Users execute an Agreement prior to receiving access to the HMIS, and complete Annual Review Training and execute a new CCHMIS User Agreement every year to maintain HMIS access (see https://caresny.org/cchmis for details).

EXEMPTIONS

This policy does not apply to Users at Vendor CHOs; these Users are regulated by the HMIS Vendor.

SECTION 5.4 DISCRETIONARY HMIS AGREEMENTS

Scope: Other agreements executed as part of the administration of the HMIS.
Applicability: HMIS Lead, CHOs.

5.4.1 MEMORANDUMS OF UNDERSTANDING (MOU) POLICY

POLICY

A Memorandum of Understanding (MOU) will allow disclosure of client-level HMIS PII for research purposes to a data recipient (individual or institution) if the research purpose of the MOU reflects an intent to benefit the homeless community. An MOU will ensure that the data recipient will employ privacy and security measures at least equal to those prescribed herein to ensure that the identity and confidentiality of all HMIS clients is protected and not disclosed. Only the minimum amount of information required to fulfill the research purpose will be disclosed, determined at the professional judgement of the HMIS Lead. No client-level HMIS PII will be released for research purposes without an adequate and executed MOU. An MOU will **not** be a substitute for approval of a research project by an Institutional Review Board, Privacy Board, or other applicable human subjects protection institution.

STANDARDS

» A Research Memorandum of Understanding must:
  a. (1) Establish rules and limitations for the processing and security of PII in the course of the project;
  b. (2) Provide for the return or proper disposal of all PII at the conclusion of the project;
  c. (3) Restrict additional use or disclosure of PII, except where required by law; and
  d. (4) Require that the data recipient formally agree to comply with all terms and conditions of the agreement.

» A Research MOU must be executed (agreed upon and signed to by all parties) before any data will be released.

» The HMIS Program Director must be the signing party for the HMIS Lead.

PROCEDURES

RESEARCH MOU OUTLINE

1. The HMIS Lead requires all Research MOUs to clearly define, at a minimum, the following information:
   a. The scope of work;
   b. The goals of the project;
   c. The responsibilities of each party;
   d. The benefit to the homeless community;
   e. A term limit for the project;
   f. The privacy and security requirements to be upheld;
   g. The data elements to be shared;
   h. How the data is to be accessed;
   i. How the data is to be used;
   j. Limitations of data use; and
   k. How the data will be securely disposed of or returned at the end of research project.

ADDITIONAL INFORMATION

A template of the research MOU is available on the HMIS Lead website https://caresny.org/cchmis.

Copies of past research MOUs are available upon request to the Director of HMIS Project and Services.

SECTION 5.5 DOCUMENT MAINTENANCE & AVAILABILITY

Scope: Maintenance and availability of contracts and agreements executed as part of the administration of the HMIS.
Applicability: HMIS Lead.

5.5.1 RETENTION & AVAILABILITY POLICY

POLICY

The HMIS Lead will retain copies of all contracts and arrangements executed as part of the administration and management of the HMIS. The HMIS Lead will ensure copies of are available for review.

STANDARDS

» The HMIS Lead must retain a copy of each executed contract and arrangement for at least seven (7) years past the date of expiration or the date the agreement is superseded.

PROCEDURES

COPIES OF DOCUMENTS

1. Blank copies of the following documents are available on the HMIS Lead website:
   a. CCHMIS User Agreements; and
   b. CCHMIS CHO Agreements.

EXECUTED AGREEMENTS OR CONTRACTS

2. Copies of executed agreements or contracts are available upon written request to the HMIS Program Director.

ADDITIONAL INFORMATION

The seven (7) year requirement is intended to match the retention period required for HMIS data:

> *"HMIS data must be stored at the central location for a minimum of seven years after the date of collection by the central coordinating body or designee of the CoC. The seven-year requirement is the current government standard for health and medical information."*[7]

[7] HMIS 2004

ARTICLE 6. DOCUMENT CONTROL & MAINTENANCE

Purpose: To ensure maintenance of the CARES Collaborative HMIS Policies & Operations Manual document by the HMIS Lead and governance parties.

SECTION 6.1 VERSION AUTHORITY

Scope: Actions to review, update, and approve this document or parts herein.
Applicability: HMIS Lead, HMIS Governance parties.

6.1.1 VERSION AUTHORITY

POLICY

Each published version and subversion of this document fully replaces all prior versions and subversions, and all future versions and subversions will likewise supersede and replace it.

SECTION 6.2 DOCUMENT CONTROL

6.2.1 VERSION POLICY

POLICY

Policies will guide the actions of all parties named within this document, and as such will require approval by the HMIS Advisory Committee before becoming effective.

STANDARDS

- A new document version must be issued following any approved revisions to any policies.
- Every new version must be numbered in increasing whole number increments.

6.2.2 SUBVERSION POLICY

POLICY

Standards and procedures are determined by the HMIS Lead and are not subject to HMIS Advisory Committee approval.

STANDARDS

- A new document subversion must be issued following revisions to standards and procedures.
- Every new subversion must be numbered in increasing one-tenth number increments after the same version number.

SECTION 6.3 MAINTENANCE

Scope: Actions to review this document or parts herein.
Applicability: HMIS Lead.

6.3.1 REVIEW & REVISION RESPONSIBILITY

POLICY

The HMIS Lead will be responsible for reviewing and updating this Document and ensuring it remains compliant with all federal HMIS requirements.

STANDARDS

- The HMIS will maintain documentation of all past versions and subversions.

6.3.2 FREQUENCY OF REVIEW & REVISION POLICY

POLICY

This document, including all associated appendices, will be reviewed at least annually and revised as necessary.

ARTICLE 7. COMMUNICATION

SECTION 7.1 GENERAL

Purpose: To ensure meaningful and appropriate communication with the HMIS Lead across all communication methods, including phone/verbal, print/written, and electronic communications.
Scope: All communication, regardless of method.
Applicability: General.

7.1.1 COMMUNICATIONS CODE OF CONDUCT

POLICY

The following rules govern all communications, and these rules are assumed to be included and to hold true within all other policies:

1. All parties will behave in a professional and respectful manner.
2. All parties will engage in only relevant and appropriate communications.
3. All parties will work in an equitable, productive, and timely manner.
4. Every reasonable effort will be made to ensure that client confidentiality is preserved.

7.1.2 HMIS LEAD CONTACT POLICY

POLICY

The HMIS Lead will be available to address questions, inquiries, and concerns that are relevant to the HMIS and are appropriate for communication.

STANDARDS

» Communications must comply with all applicable security and privacy requirements.

PROCEDURES

CONTACTING THE CCHMIS

PRIVACY/SECURITY REMINDER*: An internal HMIS HelpDesk ticket is the* ***ONLY*** *time or place you may include client-level information in a written communication without breaching confidentiality.*

EMAIL AND VOICEMAIL MESSAGES

HMIS staff contact information may be located at: https://caresny.org/cchmis/#Our-Team

1. Include the following information in all email and voicemail messages:
   a. The sender’s full name;
   b. The name of the sender’s organization;
   c. A brief description of the issue; and
   d. A return phone number and/or email address.
2. Afterhours and additional methods of contacting the HMIS team can be found at https://caresny.org/cchmis/#After-Hours

7.1.3 VEXATIOUS, MALICIOUS, OR FRIVOLOUS COMMUNICATIONS POLICY

POLICY

HMIS Lead staff will not tolerate or engage with any vexatious, malicious, or frivolous communication. Violations of this policy will be determined at the discretion of the HMIS Program Director, as will be any actions in response to a violation.

PROCEDURES

ASSESSMENT

1. Any communication thought to be vexatious, malicious, or frivolous communication sent to any HMIS Lead staff member will be referred to the HMIS Program Director for review.

RESPONSE & FURTHER ACTIONS

2. The HMIS Program Director will evaluate the situation and may
   a. Advise the offender on acceptable communication; or
   b. Direct all future communication to be completed through the HMIS Lead Program Director.
3. If a violation is severe enough, or if a violation is repeated, the HMIS Program Director may involve the Executive Director of the HMIS Lead and/or the CHO Director of the offending person to collectively evaluate the situation and determine further action.

SECTION 7.2 HMIS LEAD

Purpose: To ensure that the HMIS Lead is available and responsive to persons and parties with responsibilities to the HMIS.
Scope: HMIS Lead response to communications, attendance to community meetings, and notification to CHOs and Users or HMIS-related information and events.
Applicability: HMIS Lead.

7.2.1 HMIS LEAD RESPONSE POLICY

POLICY

The HMIS Lead will respond to appropriate communications in a timely manner.

PROCEDURES

RESPONSE

1. The HMIS Lead will respond via the method of communication used for initial contact, unless another method is requested or is more suitable to address the subject matter.
   a. Default response time frame for customer communications: 24 hours during normal business hours.
   b. Default response time frame for non-customer communications: 48 hours during normal business hours.

WEBINAR COMMUNICATION

2. Training, HelpDesk, and/or technical assistance may be facilitated via a webinar format for better assistance.
   a. Webinars will be arranged by the HMIS Lead.

EXEMPTIONS

The response time frame within this policy is superseded by all other policies that specify a different response time frame.

7.2.2 HMIS LEAD MEETING ATTENDANCE POLICY

POLICY

A member of the HMIS Lead staff will be available to attend Planning/CoC and Data Committee meetings and other HMIS-related meetings upon request.

PROCEDURES

REQUESTING HMIS LEAD ATTENDANCE AT A MEETING

1. Contact the HMIS Lead staff member of interest to set up attendance:

a. In-person attendance to local[8] meetings: Notice of at least three (3) business days is requested.
b. In-person attendance to meetings more than 50 miles outside of Albany, NY: Notice of at least thirty (30) days is requested.
c. Call-in: Notice of at least two (2) business days is requested.

7.2.3 HMIS LEAD LISTSERV NOTIFICATIONS POLICY

POLICY

The HMIS Lead will notify Users in a timely fashion of service outages, data updates, new forms for their use, and other important HMIS administrative information via the HMIS Listserv. The HMIS Listserv will only be for the stated purpose (HMIS-related information dissemination) and the contact information it contains will never be disclosed or shared.

PROCEDURES

INITIAL LISTERV SUBSCRIPTION

1. All new Users are subscribed for the HMIS Listserv when they receive their User credentials.

SECTION 7.3 USERS

Purpose: To outline important communication policies for Users.
Scope: User questions regarding HMIS function, issues, and client-level data.
Applicability: Users.

7.3.1 HMIS HELPDESK

POLICY

Users will use the HMIS HelpDesk to ask questions about HMIS data collection, data entry, HMIS use, and to transmit any client-level data. Users will never transmit client-level data outside of the HMIS HelpDesk.

STANDARDS

» Users must use the HMIS HelpDesk to transmit any client-level information.

7.3.2 HMIS LISTSERV SUBSCRIPTION POLICY

POLICY

Active Users and CHO administrative staff will subscribe to the HMIS Listserv to receive important communications regarding the HMIS. The HMIS Lead will not be held responsible for otherwise informing Users of information it disseminates via the Listserv nor for any adverse events (or the mitigation of such events) that occur due to Users voluntarily unsubscribing to the Listserv and not receiving information.

PROCEDURES

SUBSCRIBE

1. Individuals, even non-Users, can subscribe to receive updates using the form located on the HMIS Lead's website, available on the User Training page (https://caresny.org/cchmis).
2. Contact an HMIS Customer Service Representative if you experience issues.

UNSUBSCRIBE

3. Users can click the "Unsubscribe" link on the bottom of every HMIS Listserv email to be removed from the list.

ADDITIONAL INFORMATION

Users are strongly encouraged to remain subscribed to the HMIS Listserv, as it is the primary method of communication used by the HMIS Lead regarding the HMIS.

[8] Local: within a 50-mile radius of the HMIS Lead main office in Albany, NY. See exact address in Directory.

ARTICLE 8. TRAINING

Purpose: To describe the HMIS training plan provided by the HMIS Lead and provide the expectations and requirements of Users, with respect to the attendance to and completion of HMIS training.

SECTION 8.1 HMIS LEAD

Scope: Training provided by the HMIS Lead.
Applicability: HMIS Lead.

8.1.1 TRAINING PROGRAM POLICY

POLICY

The HMIS Lead will develop and maintain a training program and resources to provide to Users at CHOs that will facilitate high levels of data completeness and data quality. The HMIS Lead will maintain and update the training program and resources to reflect current HMIS data standards and will ensure availability of the training program and resources to all Users. The HMIS Lead will provide standard HMIS training sessions to CHOs at no extra cost.

STANDARDS

» The HMIS Lead must offer training sessions at reasonable intervals.

» Training on data entry must be conducted using training programs within the HMIS Lead database that are separate from the rest of the HMIS data and are NEVER included in any HMIS reports.

PROCEDURES

STANDARD TRAINING

1. The HMIS Lead offers standard, regularly scheduled training (*Table 2*) at no cost to User at CHOs.
   a. Training sessions are offered on-line (self-guided and webinar) and in-person.
   b. Trainings sessions may range from 1- to 4-hours
   c. Unless otherwise specified, in-person training occurs at the HMIS Lead main office in Albany, New York.

Table 2. Currently offered standard training sessions. Starred (*) training sessions are required.

SESSION NAME/TITLE	METHOD	AVAILABILITY	DESCRIPTION	LENGTH
*NEW USER TRAINING	Online	N/A	Comprehensive introduction to the HMIS database and its use including: navigation, data elements, security and privacy, and basic data entry functions including admissions, information updates, and discharges.	3-4 hours
	Live, in-person or webinar	By Request/As new organizations join the CCHMIS		
*ANNUAL REVIEW TRAINING (PRIVACY AND SECURITY)	Online	Annual	Refreshes Users knowledge and awareness of privacy and security as well as any other important AWARDS or program data updates.	1-2 hours
	Live, in-person or webinar	Annual		
ACCESS PERMISSIONS/ADVANCED USER/AGENCY HMIS ADMINISTRATOR TRAINING	Live, in-person or webinar	By Request/As needed due to information updates	Required for CHO Agency Administrators (or other Users, as appropriate) to gain permissions to perform advanced functions.	1-2 hours
RECURRING USER GROUPS TRAINING	Live, in-person or webinar	By Request/As needed due to	Occurs in response to Data Standards changes; Users will be notified of availability via the HMIS Listserv.	1 hour

		information updates		
EMERGENCY SHELTER TRAINING	Live, in-person or webinar	As-needed to train all ES staff	Training specifically for Emergency Shelter staff regarding on data collection	1 hour
PROGRAM DIRECTOR TRAINING	Live, in-person or webinar	By Request/As needed due to information updates	Required for new Program Directors or Agency HMIS Administrators to receive the associated permissions, including access to all CHO program data to for running CHO-level data quality reports.	1-2 hours

ONLINE RESOURCES

1. The HMIS Lead maintains a resource library of documents and videos that provide detailed instructions for common processes Users may need to complete.
   a. Resources are available on the HMIS Lead website: https://caresny.org/cchmis
   b. Available training topics include: Intake/Discharge/Updates to HMIS records; Universal data element guidance; how to run specific reports and read results; and how to monitor data quality.
   c. The resource library is added to regularly, and existing resources are continuously updated to reflect any changes in data standards or processes.

8.1.2 ANNUAL REVIEW TRAINING POLICY

POLICY

The HMIS Lead will provide Annual Review Training to all Users at CHOs and will cover security and privacy measures and any HMIS updates from the past year.

STANDARDS

» Annual Review Training must include a security and privacy policy review.

» Annual Review Training must be made available to all Users at all CHOs.

» Annual Review Training must include execution of a new confidentiality agreement with a deadline for completion.

PROCEDURES

ANNOUNCEMENT/COMMUNICATION

1. The HMIS Lead will provide all information pertaining to the Annual Review Training to Users via the HMIS Listerv (dates/times, links to training, documents, reminders, and deadlines._
   a. Training will be conducted at multiple times and will be available via multiple methods (including an online option) to accommodate all Users.
   b. An updated CCHMIS User Agreement will be provided along with the training.
2. Users will be reminded of the training and CCHMIS User Agreement completion deadline via the HMIS Listerv.

SECTION 8.2 USERS

Scope: Users attending HMIS training sessions.
Applicability: Users.

8.2.1 USER TRAININGS POLICY

POLICY

Users will complete all required training and all training requested of them by the HMIS Lead. Users will follow all procedures regarding attending and requesting training.

PROCEDURES

ATTENDING STANDARD TRAINING

1. Users must register in advance to attend an in-person standard training session.
    a. Unless otherwise indicated, trainings occur at the HMIS Lead office (see https://caresny.org for location details).
    b. Requests for remote access (webinar) to a standard training session must be made at least one (1) full business day in advance of the scheduled training. A microphone and speaker system or a regular telephone and a computer is required.
2. Scheduled attendees must notify the HMIS Lead prior to 5pm the business day before the training to cancel their attendance, or the No-Show Policy will apply.

REQUESTING CUSTOM, ON-SITE OR SUPPLEMENTARY TRAINING

1. Users may contact an HMIS Customer Service Representative to schedule a custom, private training:
    a. In-house sessions less than 4 hours in length will be provided at no cost.
    b. Other sessions may incur to fees, such as:
        i. Training not during standard business hours;
        ii. Training requiring more than 4 hours; or
        iii. Training on-site (at a CHO) that requires HMIS Lead travel.
2. Send requests for training via email to an HMIS Customer Service Representative and include the following:
    a. The desired method of training;
    b. The desired date and time (or range of dates/times for training;
    c. The number of persons interested in the training; and,
    d. The desired training session or topics (if not a standard session).
3. Training requests will be evaluated and responded to with further instructions.

NONCOMPLIANCE/REMEDIAL TRAINING

1. Users that fall under noncompliance with respect to User access and User training requirements will be subject to remedial training.
2. The remedial training session(s) required will be prescribed at the HMIS Lead's discretion staff.
3. Remedial training **must** be completed via an instructor-led training, by:
    a. Attending a previously scheduled session; or
    b. Custom request
4. Dependent upon the length of the training, this may be subject to fees.
5. User access will remain revoked until the User completes the remedial training prescribed by HMIS Lead staff.

ANNUAL SECURITY & PRIVACY TRAINING

1. The HMIS Lead will inform Users when the Annual Review Training is available via the HMIS Listserv and provide a deadline date for completion.
2. Users must complete the training by the deadline to retain active status of their User account.

REMOTE/OFF-SITE ACCESS TO TRAINING

1. Users can request remote access to any scheduled in-house training sessions via webinar.
    a. Requests must be made at least one (1) full business day in advance of the training.
    b. Remote access requires either a microphone and speaker system, or a regular telephone in conjunction with a computer.
2. Contact an HMIS Customer Service Representative to request remote access.

8.2.2 USER TRAINING PARTICIPATION POLICY

POLICY

A User will complete all required training to receive and maintain User credentials, including training requested of them by the HMIS Lead. A User that fails to complete required training to a satisfactory level will have their User credentials revoked.

STANDARDS

- » Users must be computer-literate prior to attending any User training.
- » Users must register in advance for in-person training sessions.
- » Users must complete the Annual Review Training every year to retain active User status.

PROCEDURES

COMPLETION OF TRAINING

1. Users complete a training as described below (*Table 3*).

Table 3. Requirements for satisfactory completion of training.

SESSION	REQUIREMENT
LIVE TRAINING	Attendance to the full duration of a session
ONLINE TRAINING	A score of 80% or higher on applicable online training quiz

2. Users that do not attend the full training session may be asked to repeat the session or to complete the session via a private training session.
3. Users that do not achieve satisfactory completion of a training may be required to repeat the session.

ANNUAL REVIEW TRAINING

1. All Users must complete Annual Review Training and execute a new CCHMIS User Agreement when requested by the HMIS Lead.
    a. Users that fail to complete the training and submit a new agreement by the deadline date will have their User credentials (for accessing the HMIS) deactivated until they do so.

EXEMPTIONS

Exemptions to this policy may be granted by the HMIS Program Director or HMIS System Administrator.

8.2.3 TRAINING SESSION CANCELLATIONS & NO-SHOW POLICY

POLICY

Users registered for a training session with the HMIS Lead are expected to attend or to properly cancel their attendance. At the discretion of the HMIS Lead, no-shows to a training session may have their User account deactivated until the missed training is completed.

Please note*: This policy applies to* <u>*scheduled*</u> *training sessions, both in-person and webinar. It does not apply to self-administered online video training.*

PROCEDURES

CANCELLING ATTENDANCE

1. Scheduled attendees must notify the HMIS Lead Agency prior to **5pm the business day before** the training.

PROCEDURES

NO-SHOW TO SCHEDULED, NON-REQUIRED TRAINING

2. The User may still be subject to service fees for the missed training, to be determined at the HMIS Lead's discretion System Administrator.

NO-SHOW TO REQUIRED TRAINING

3. The User will be considered noncompliant as of the date of the missed training and have their User access revoked on that date or shortly thereafter.

NO-SHOW ACCESS RESTORATION

4. User access will be restored once the User completes the training that was missed by:
   a. Regularly scheduled training session: If the training was a regularly scheduled training, the User may wait until the next time the training is offered, or;
   b. Private training session: If the training was originally a private session or if the training is no longer offered, it must be requested as a private training and will be subject to CARES' hourly fee (see the Appendix) plus any travel expenses, if required.

EXEMPTIONS

Exemptions to this policy may be granted by the HMIS Program Director or HMIS System Administrator.

ARTICLE 9. GRIEVANCES

Purpose: To ensure there is a way to give comments or raise complaints regarding the HMIS, and that these matters are dealt with promptly and fairly.

SECTION 9.1 CLIENTS

Scope: Grievances of clients regarding the HMIS.
Applicability: HMIS Lead, CHOs, Clients.

9.1.1 CLIENT GRIEVANCE POLICY

POLICY

Any client of a CHO may submit a grievance to the HMIS Lead if they believe any of their rights as an HMIS client, as specified in the CCHMIS Client Inclusion Disclosure and Release of Information Form, have been violated and not adequately addressed by the CHO. Grievances will not bias the service provision or treatment of a client by a CHO. Grievances do not constitute legal action and HMIS Lead does not provide legal services

STANDARDS

- » Clients must follow CHO procedures for grievances prior to submitting a grievance to the HMIS Lead.
- » Grievances must be submitted in writing to be considered an official complaint.
- » Phone calls regarding grievances may be recorded for recordkeeping purposes.

PROCEDURES

SUBMISSION

1. As an HMIS client, if you believe that your rights as specified in the CCHMIS Client Inclusion Disclosure and Release of Information Form have been violated at your provider (CHO):
   a. Follow the grievance procedures at your provider (CHO) that you believed violated your rights.
2. If you are not satisfied with how your grievance was answered by your provider (CHO), you may then submit a grievance to the HMIS Lead in writing via the CCHMIS Grievance form (available via the HMIS Lead Website: https://caresny.org/cchmis).

RESPONSE & FURTHER ACTIONS

3. The HMIS Lead will respond to your grievance within thirty (30) days of receipt.
   a. The HMIS Lead will attempt a voluntary resolution of the grievance by ensuring that your provider (CHO) is compliant with all HMIS requirements.
   b. The HMIS Lead will notify you of any and all actions taken to resolve your grievance via phone or email.
4. You may request to have documentation of the grievance included in your records at your provider (CHO).

SECTION 9.2 CHOS

Scope: Grievances of Agency HMIS Administrators regarding the administration of the HMIS to the HMIS Lead.
Applicability: Agency HMIS Administrators.

9.2.1 CHO GRIEVANCE POLICY

POLICY

A grievance may be submitted to the HMIS Lead, on behalf of a CHO, regarding the administration of the HMIS.

STANDARDS

- Grievances do not constitute legal action and HMIS Lead does not provide legal services.
- Grievances regarding the administration of the HMIS must be submitted by the Agency HMIS Administrator.
- Grievances must be submitted in writing to be considered an official complaint.
- Phone calls regarding grievances may be recorded for recordkeeping purposes.

PROCEDURES

SUBMISSION

1. Agency HMIS Administrators are encouraged to contact the HMIS Program Director to work towards a collaborative resolution regarding any complaints with the administration of the HMIS.
2. If the resolution is insufficient, the Agency HMIS Administrator may submit a complaint to the Executive Director of the HMIS Lead in writing via the CCHMIS Grievance form (available via the HMIS Lead website: https://caresny.org/cchmis).

RESPONSE & FURTHER ACTIONS

3. The Executive Director of the HMIS Lead will respond to your grievance within 30 days of receipt in writing, via print or email.
4. As appropriate, the complaint may be brought to the CoC Lead(s) and/or the HMIS Advisory Committee for further review.
5. You will be notified of all actions taken in response to your grievance.

ARTICLE 10. MONITORING

Purpose: To ensure CHOs, who process HMIS protected identifying information (PII), are adequately and correctly implementing privacy and security measures for HMIS and in compliance with all applicable law.

SECTION 10.1 MONITORING

Scope: Monitoring of all processes involving HMIS use at CHOs, including the operations of the HMIS Lead.
Applicability: All CHOs, including the HMIS Lead.

10.1.1 HMIS MONITORING REQUIREMENT POLICY

POLICY

All CHOs, including the HMIS Lead, will undergo regular review to ensure compliance with, and full implementation of, all applicable HMIS policies and standards.

10.1.2 HMIS LEAD CHO MONITORING POLICY

POLICY

The HMIS Lead will monitor CHOs regularly for compliance, particularly with security and privacy measures, and CHOs will comply with all HMIS Lead requests to enable the HMIS monitoring process. Refusal or deliberate obstruction of the monitoring process will not be tolerated and will be treated as noncompliance.

STANDARDS

- » HMIS monitoring for CoC-funded programs must be conducted with a site visit at least once annually.
- » HMIS monitoring for non-CoC-funded programs must be conducted with a site visit or remotely at least once annually.
- » HMIS monitoring must include completion of a security checklist ensuring that security standards are implemented in accordance with the Security Plan.
- » CHOs must comply with all HMIS Lead requests to facilitate HMIS Monitoring.

PROCEDURES

TECHNICAL ASSISTANCE FOR ANNUAL HMIS MONITORING

1. A CHO may request monitoring technical assistance from the HMIS Lead at any time.
   a. Assistance may be provided in the form of a phone or in-person meeting between the HMIS Lead and the CHO to review the monitoring materials.

SCHEDULING

2. The HMIS Lead will contact the CHO via email to schedule monitoring, and this email will include:
   a. Expectations and CHO requirements for monitoring;
   b. HMIS Monitoring materials, including:
      i. HMIS Monitoring Project Information Forms for each project;
      ii. HMIS CHO Security Certification Form;
      iii. HMIS Monitoring Security & Privacy Checklist; and
      iv. HMIS Required Document Checklist.
3. The HMIS, with the CHO, will determine a suitable date for site visit monitoring OR a due date if remote monitoring is permissible.

ANNUAL HMIS MONITORING – SITE VISIT

4. For site visit monitoring, a CHO is expected to prepare for monitoring by:
   a. Having the Agency HMIS Administrator available for the date and time monitoring is scheduled;
   b. Having all paperwork complete and copies available for the HMIS Lead, as necessary; and

    c. Complying with all HMIS Lead requests for the duration of the site visit.

5. The HMIS Lead will record all findings, including instances of noncompliance, on the HMIS Monitoring Form.

ANNUAL HMIS MONITORING – REMOTE

6. The CHO is expected to complete all forms and provide all required and appropriate information to the HMIS Lead by the due date.

ANNUAL HMIS MONITORING REVIEW OF RESULTS

7. Completed monitoring forms will be reviewed post-monitoring by the HMIS Lead.
    a. Instances of noncompliance will be addressed as per CHO Monitoring Noncompliance Policy.
8. A monitoring report will be submitted by the HMIS Lead to the CoC Board for improved oversight and transparency and may also be shared with HMIS Lead and/or CoC governing bodies such as the Collaborative Applicant, CoC Lead, HMIS Advisory Committee, or Data Committee for the community.

10.1.3 HMIS LEAD SELF-MONITORING POLICY

POLICY

The HMIS Lead will conduct a security review of all on-site HMIS Lead operations to ensure compliance and full implementation of all applicable policies and standards.

STANDARDS

- HMIS monitoring must be conducted at least once a year.
- HMIS monitoring must include completion of a security checklist ensuring that security standards are implemented in accordance with the Security Plan.

PROCEDURES

MONITORING

1. HMIS Lead Self-Monitoring is conducted annually, at the HMIS Lead's discretion.

RESULTS

2. A copy of the most recent HMIS Lead self-monitoring results may be requested from the HMIS Lead's designated HMIS Security Officer.

ARTICLE 11. NONCOMPLIANCE

Purpose: To ensure appropriate actions are taken in situations where an individual or entity fails or refuses to comply with any policies and procedures herein.

SECTION 11.1 USERS

Scope: Any User action that violates User requirements as described herein or as otherwise agreed to in writing.
Applicability: CHOs, HMIS Lead, Users.

11.1.1 USER TRAINING NONCOMPLIANCE POLICY

POLICY

Noncompliant Users will have their User access revoked by the HMIS Lead until compliance is demonstrated. The HMIS Lead reserves the right to require Users to complete additional training prior to restoring User access.

STANDARDS

» Users requested to complete training must complete the training to a satisfactory level to have their User access restored.

PROCEDURES

REVIEW OF NONCOMPLIANCE

3. The HMIS Lead will revoke the User's HMIS access by default at the time the User noncompliance is determined.
4. The HMIS Lead will contact the Agency HMIS Administrator of the User that was noncompliant to inform how the User can demonstrate and come back into compliance (see below).

DEMONSTRATION OF COMPLIANCE

5. User compliance may be demonstrated by one of the following processes:
   a. If a failure to maintain current documentation: Complete and send in proper documentation. Access will be regained as soon as documentation is received.
   b. If a failure to complete required training on time or successfully: Successful completion of required training at the next available time or via a Custom Training session (to which additional fees may apply).
   c. If persistent poor data entry: Completion of remedial training as prescribed by the HMIS Lead).
      i. This training must be completed via a live training session (in-person or via webinar).

RESTORATION OF USER ACCESS

6. User access will be restored for the individual once compliance is demonstrated.

11.1.2 USER PRIVACY & SECURITY NONCOMPLIANCE POLICY

POLICY

Users that violate HMIS security and/or privacy policies will have their User access revoked by the HMIS Lead immediately upon discovery. The HMIS Lead reserves the right to indefinitely revoke a User's access in response to a breach of client confidentiality.

PROCEDURES

REVIEW OF NONCOMPLIANCE

7. The HMIS Lead System Administrator and/or the HMIS Program Director will review all situations where a User may have been noncompliant to determine if noncompliance had occurred or not.
8. The HMIS Lead will report to the Agency HMIS Administrator of the User's CHO with a conclusion within three (3) business days:

a. If the HMIS Lead concludes that noncompliance **had** occurred: The HMIS Lead will have a discussion with the Agency HMIS Administrator of the User that was noncompliant to discuss further action.

b. If the HMIS Lead concludes that noncompliance **had not** occurred: The HMIS will notify the individual who reported the situation, and the revoked User access will be restored within one (1) business day.

c. If the HMIS Lead **could not definitely conclude** that noncompliance had or had not occurred: The HMIS will notify the individual who reported the situation and request additional information or a follow-up conversation.

d. If a failure to maintain client confidentiality: the HMIS Program Director will have a conversation with the CHO of the User, and additional action will be as per the CHO's noncompliance and sanctions policies.

FURTHER ACTION/COMPLIANCE

9. If, and the appropriate method for, a User to come back into compliance and obtain restored User access to the HMIS will be the discretion of the HMIS Lead Program Director.

11.1.3 CHO NONCOMPLIANCE POLICY

POLICY

A CHO action that violates CHO requirements as described herein or as otherwise agreed to in writing will be considered an act of noncompliance. A CHO will be held responsible for timely correction of any instances of noncompliance with HMIS policies and procedures. A correction plan may be required to demonstrate compliance, determined at the HMIS Lead's discretion Program Director.

STANDARDS

» Any corrective activity to demonstrate compliance must have written documentation (e.g., meeting minutes, monitoring forms, emails, or letters.)

PROCEDURES

REVIEW OF NONCOMPLIANCE

1. If noncompliance is discovered by the HMIS Lead (i.e., during monitoring):
   a. The HMIS Lead will contact the Agency HMIS Administrator within ten (10) business days of monitoring to discuss the instance(s) of noncompliance and to form a plan for correction.
2. If noncompliance is reported to the HMIS Lead:
   a. The HMIS System Administrator and/or the HMIS Program Director will review the situation to determine if the CHO is noncompliant.
3. The HMIS Lead will respond to the report with a conclusion within three (3) business days:
   a. If the HMIS Lead concludes the CHO is **noncompliant**: The HMIS Lead will have a discussion with the Agency HMIS Administrator (as above).
   b. If the HMIS Lead concludes the CHO is **compliant**: The HMIS will notify the individual who reported the situation. No further action will be taken.
   c. If the HMIS Lead **could not definitely conclude**: The HMIS will notify the individual who reported the situation and request additional information or a follow-up conversation.

DEMONSTRATION OF COMPLIANCE

4. At the discretion of the HMIS Program Director, compliance may be demonstrated by one of the following processes:
   a. If a failure to maintain current documentation: Complete and send in proper documentation.
   b. If a failure to implement privacy or security measures or protocols: Development of a correction plan with the HMIS Lead.
   c. If a consistent failure to meet data quality benchmarks: Development of a correction plan with the HMIS Lead.

CORRECTION PLAN

5. A written correction plan will include, at a minimum:
    a. Requirements for compliance;
    b. Implementation steps;
    c. HMIS Lead oversight and right to deactivate any User access at any time; and
    d. A schedule of additional HMIS Monitoring visits to ensure compliance.

FAILURE TO COMPLETE CORRECTION PLAN

1. If a correction plan is not followed, or there is not adequate improvement, the HMIS Program Director may do any of the following:
    a. Report the CHO to the CoC Lead and/or the funding entity (e.g., HUD or OTDA);
    b. Require the Agency HMIS Administrator to meet with a representative of the CoC and/or the CCHMIS to create a more extensive action plan;
    c. Require monthly monitoring visits for at least six months.
    d. Suspend the project(s) of the CHO in the HMIS, if they are not required to participate in HMIS, until corrective action is taken.
2. If a CHO required to participate in HMIS continues to be out of compliance:
    a. Its projects will be suspended within the CCHMIS;
    b. Technical Assistance may be sought from the funding entity (OTDA, federal partners, and/or HUD);
    c. Suspended program will be listed as ‘Not Participating’ on the CoC Housing Inventory Chart and in any renewal applications within the CoC Grant Application.

11.1.4 UNLAWFUL NONCOMPLIANCE POLICY

POLICY

Any violation of HUD regulations and/or action against the law involving the HMIS will be reviewed by the HMIS Lead Program Director. The HMIS Lead reserves the right to elevate the situation to the CoC for determination of unlawful noncompliance and further action. Further actions will be determined at the discretion of the CoC, as per the HMIS Proposed Rule of 2011 Subpart F—Sanctions (§ 580.51) “the program regulations for the programs that fund the HMIS activities contain the sanctions for noncompliance with this part.”.

PROCEDURES

REVIEW OF NONCOMPLIANCE

1. Any suspected instance of unlawful noncompliance will be reviewed by the HMIS Lead Program Director.
    a. The HMIS Lead Executive Director may be included in the discussion.
2. If an instance of unlawful noncompliance is reasonably suspected, the HMIS Lead will elevate the situation to the CoC.

FURTHER ACTION

3. Determination of unlawful noncompliance and further actions will be determined at the discretion of the CoC, including any disciplinary actions.

ARTICLE 12. CCHMIS DATA QUALITY PLAN

Purpose: Data completeness and quality are integral to the relevance and usefulness of HMIS, and as such are accounted for in all required reports to HUD through specific quality measures (and indirectly, through how accurately the community is described by the data). The measures described in this plan are intended to ensure the completeness, accuracy, timeliness, and consistency of data in the HMIS;[9] and support CHOs in their efforts to reach and exceed quality benchmarks and, in general, to achieve the highest quality data possible.

SECTION 12.1 HMIS DATA COLLECTION & ENTRY

Scope: HMIS data collection at CHOs.
Applicability: CHOs and Users.

12.1.1 REQUIRED COLLECTED DATA POLICY

POLICY

A CHO participating in a local HMIS will be required to collect all Universal Data Elements (UDEs) from all homeless clients seeking housing or services for their projects in HMIS, regardless of program type or funder and including projects that are not federally funded, including date of birth, race, ethnicity, gender, veteran's status and Social Security Number (SSN). A CHO will also collect all Program Specific Data Elements (PSDEs) when they are required by a non-HUD Federal Partner. CHOs will follow all guidelines, standards, and requirements for HMIS data collection as set forth by HUD and each Federal Partner.

STANDARDS

- CHOs must collect all UDEs to the best of their ability.
- CHOs must collect all PSDEs that apply to their projects to the best of their ability.

PROCEDURES

REQUIRED DATA ELEMENTS

1. CHOs will collect the HMIS information appropriate to the program, project, and client, for all persons served by projects required to participate in the HMIS.
    a. Universal Data Elements and common Program-Specific Data Elements are provided below (Table 4. HMIS data elements.*Table 4*).
        i. Common PDSEs are collected for most programs.
    b. Program manuals for the HMIS provide the best information on data collection.

Table 4. HMIS data elements.

UNIVERSAL DATA ELEMENTS	COMMON PROGRAM-SPECIFIC DATA ELEMENTS:
3.1 Name	4.2 Income and Sources
3.2 Social Security Number	4.3 Non-Cash Benefits
3.3 Date of Birth	4.4 Health Insurance
3.4 Race	4.5 Physical Disability
3.5 Ethnicity	4.6 Developmental Disability
3.6 Gender	4.7 Chronic Health Condition
3.7 Veteran Status	4.8 HIV/AIDS
3.8 Disabling Condition	4.9 Mental Health Problem
3.10 Project Start Date	4.10 Substance Abuse
3.11 Project Exit Date	4.11 Domestic Violence
3.12 Destination	4.12 Contact

[9] From § 580.37 Data Quality Standards and Management, HMIS Proposed Rule of 2011.

3.15 Relationship to Head of Household	4.13 Date of Engagement
3.16 Client Location	4.14 Bed-Night Date
3.20 Housing Move-in Date	4.18 Housing Assessment Disposition
3.917 Living Situation	

ADDITIONAL INFORMATION

Please see HUD's most recent HMIS Data Manual for instructions on how to collect data appropriately and accurately into the HMIS, and/or the HMIS Lead website, https://caresny.org/cchmis, for additional trainings and resources.

Data quality is part of HMIS Monitoring.

12.1.2 MISSING DATA RESPONSE OPTIONS POLICY

POLICY

Data will be collected from clients as per the Client Self-Reported Data Policy. "Client refused" and "client doesn't know" responses will be used to reflect that a client refused to respond to, or did not know the answer to, an asked question. CHOs will not assume or use these answers if they did not ask the client to provide the information first. The response of "data not collected" will not be used in place of, or to circumvent, asking a client for information.

STANDARDS

- CHOs must ensure that every client is asked for **ALL** required HMIS data.
- CHOs must ensure client HMIS information is collected and entered as the client provides it.
- CHOs must make every effort to collect all required information and prevent "data not collected" data entry.
- CHOs must make efforts to reduce client refusals of information.

ADDITIONAL INFORMATION

Client refusals should be addressed as per the HUD 2022 Data Standards Manual:

> *"At a national level, in every project type, a majority of clients are willing to provide identifying information. If a project is experiencing a high rate of client refusals as compared to similar projects, CoCs should consider implementing trainings around interviewing or trust-building techniques to support client engagement. A deeper engagement with clients may lead to more rapid movement off the street and placement in housing, consistent with meeting federal goals to end homelessness and improvement on HUD's System Performance Measures. "*

12.1.3 DATA ENTRY POLICY

POLICY

For data to be meaningful across program sites, data must be entered and updated in an accurate, consistent, and timely manner in the HMIS. Only trained and authorized Users will enter data into the HMIS at CHOs, and Users will comply with all requirements as provided within the CCHMIS User Agreement.

STANDARDS

- Users must follow the requirements pertaining to data collection and data entry within all HMIS program manuals and as per the CCHMIS User Agreement.
- Users must refer to the CCHMIS Data Quality Plan Appendix 19.4 for complete Data Quality Expectations and Benchmarks.
- Users must use their personal User account for all data entry to ensure accountability for data entry.

PROCEDURES

DATA ENTRY

1. All required data (*Table 4*) will be collected at all required time-points in a client's service history, as per the most recent HMIS Data Standards (see *HUD 2022 HMIS Data Standards Manual.* for an overview of time-points).

Table 5. Data collection/entry time-points in a client's service history.

DATA	COLLECTION POINT
Intake/entry	At the time of project admission
Updates	At any point (optional)
Annual assessments	At yearly intervals, +/- 30 days from the intake date (regardless of when the last assessment was)
Aging into adulthood	At a client's birthday aging to 18 years old (as required)
Discharge	At the time of project discharge
Post-discharge	After discharge (optional)

2. Data entry/updates to the HMIS will occur in timely manner.
   a. Real-time data entry, or as close as possible, is strongly recommended.
   b. Up to 5 days is permissible after data collection for data entry into HMIS without penalty to data quality.
3. Progress notes and contact logs will remain open for data entry for a specific length of time.
   a. Time-frame will be established individually for each agency.
   b. After 2 weeks, backdating permissions must be requested via an HMIS HelpDesk request sent from the Agency HMIS Administrator.

USER ISSUES WITH DATA ENTRY

4. All issues concerning data entry should be addressed via an HMIS Helpdesk ticket or an HMIS Training request.
   a. Questions regarding specific client and client data MUST be transmitted via an HMIS Helpdesk ticket.

EXEMPTIONS

A longer time frame for backdating may be allowed at the discretion of the HMIS System Administrator.

ADDITIONAL INFORMATION

Please see HUD's most recent HMIS Data Manual for instructions on how to enter data appropriately and accurately into the HMIS, and/or the HMIS Lead website, https://caresny.org/cchmis , for additional trainings and resources.

12.1.4 ELECTIVE ADDITIONAL DATA ELEMENTS POLICY

POLICY

A CHO or a Continuum of Care may develop elective data elements to collect assessment, service tracking, and/or outcome information in more detail than required by the uniform HMIS standards. As per federal rules, the collection of additional data within the HMIS is subject to privacy and fair housing laws and practices.

ADDITIONAL INFORMATION

There are no HMIS-related penalties for not collecting elective data elements (as they will not be included in any reporting); however, a CHO or a Continuum may unofficially "require" collection by implementing self-monitoring processes and other reinforcements for the collection of elective data elements.

SECTION 12.2 PROJECT-SPECIFIC HMIS DATA POLICIES

Purpose: Extra guidance for Support Services Only or Emergency Shelter projects to acknowledge the situational challenges to data collection this type of project often presents.
Scope: Operation of Support Services Only (SSO) or Emergency Shelter (ES) projects at CHOs.
Applicability: CHOs and Users.

12.2.1 SUPPORT SERVICES ONLY DISCHARGE POLICY

POLICY

CHOs that operate Support Services Only (SSO) projects will create a policy for their Users that will exit clients from these projects if the client has been inactive for more than 90 days.

STANDARDS

» CHOs with SSO projects must have a policy for exiting clients after 90 days.

ADDITIONAL INFORMATION

Adherence to this policy is reviewed via data quality review within the HMIS Monitoring process.

12.2.2 EMERGENCY SHELTER INTAKE POLICY

POLICY

CHO staff that operate Emergency Shelter (ES) projects will collect **all** Universal Data Elements (UDEs) from clients at the time of intake, to the best of their ability. If processing a readmission for a client, CHO staff that operate Emergency Shelter (ES) projects will review any missing data from previous intakes and discharges with the client and will updates client records accordingly.

STANDARDS

» Client intake data collection must be conducted within twelve (12) hours of arrival at adult single shelters.

» CHO staff must open and saved the previous discharge record for all readmissions – even if no changes are made.

PROCEDURES

READMISSION

1. During a readmission, ES staff at CHOs should review previous intake(s) with the client to fill in any missing UDEs.
    a. The Prior Living Situation section of previous intake(s) with the client to ensure this data element is correct and updated (this data element captures information regarding previous episodes of homelessness, and thus informs the Chronic Homeless designation for the consumer.)
2. During a readmission, CHO staff MUST review previous discharge record(s)with the client to ensure a Destination was recorded.
    a. If “No Exit Interview Completed”, Client Doesn’t Know”, or “Client Refused” was recorded, CHO staff should update the record by asking the consumer where they went after they left the shelter last time.

ADDITIONAL INFORMATION

Universal Data Element **Prior Living Situation** is important because this data element captures information regarding previous episodes of homelessness, and thus informs the Chronic Homeless designation for the consumer.)

Universal Data Element **Destination** at discharge is vital to the relevancy of HMIS data, used in multiple areas of the CoC process including: System Performance Measures, LSA, Grant writing, CoC Grant Application, Vulnerability Index creation and scoring, Strategic Planning and funding allocation.

Training and workflow consultation opportunities are available to all shelters at no additional cost by contacting the HMIS Lead.

12.2.3 EMERGENCY SHELTER STAFF TRAINING POLICY

POLICY

CHO staff that operate Emergency Shelter (ES) projects will be offered specialized training from the HMIS Lead at no additional cost and may be required to take part in such training at the discretion of the HMIS System Administrator. ES staff will follow the Additional Information provided to them within Emergency Shelter training and by the HMIS Lead staff in general to provide the best quality data possible.

STANDARDS

» ES staff at CHOs must complete all specialized training requested of them by the HMIS Lead.

SECTION 12.3 DATA QUALITY BENCHMARKS

Scope: Setting data quality requirements for CHOs and CoCs.
Applicability: HMIS Lead.

12.3.1 DATA QUALITY BENCHMARKS FOR THE COC POLICY

POLICY

The HMIS Lead will set required data coverage benchmarks for the Continuum of Care to meet.

STANDARDS

» The HMIS Lead must create data quality benchmarks for the CoC.

» Lodging and nonlodging projects must have different benchmarks.

PROCEDURES

COVERAGE BENCHMARKS

1. The data of a Continuum of Care is evaluated against the benchmarks in *Table 6*.

Table 6. Benchmarks for CoC data quality.

MEASURE OF DATA QUALITY	CALCULATION	REQUIRED % COVERAGE
Minimum Bed Coverage Rates	The level of lodging project participation in a Continuum of Care's HMIS	85%
Service-Volume Coverage Rates	The level of nonlodging project participation in a Continuum of Care's HMIS.	85%

12.3.2 DATA QUALITY BENCHMARKS FOR CHOS POLICY

POLICY

The HMIS Lead will create and enforce data quality benchmarks for CHOs to ensure that the quality of HMIS data meets or exceeds federal requirements and will adjust benchmarks as necessary to reflect any changes in federal requirements or guidance. Different project types will have different benchmarks due to the disparate circumstances of the populations that utilize different homeless services

STANDARDS

» The HMIS Lead must create data quality benchmarks for CHOs.

» Lodging and nonlodging projects must have different benchmarks.

PROCEDURES

BENCHMARKS

1. The data in HMIS for EACH project at a CHO is evaluated against applicable benchmarks (See *Table 7*).

Table 7. Data quality benchmarks.

		CALCULATION	REQUIRED DATA QUALITY (SEPARATED INTO HMIS PROJECT TYPES)

MEASURE OF DATA QUALITY	PROGRAM APPLICABILITY		PERMANENT HOUSING	TRANSITIONAL HOUSING	HOMELESSNESS PREVENTION	EMERGENCY SHELTER	OUTREACH (Engaged clients only)
Timeliness of Entry	Evaluated for all projects	Length of time between HMIS data collection and HMIS data entry	< 5 business days	< 5 business days	< 5 business days	< 5 business days	< 5 business days
Universal Data Element Missing or Null	Evaluated for all projects	% of records missing UDE (each UDE is evaluated individually)	< 2%	< 2%	< 2%	< 5%	< 5%
Program-Specific Data Element Missing or Null	Program-specific; data elements as required by funding source	% of records missing required PSDE; (each PSDE is evaluated individually)	< 2%	< 2%	< 2%	< 5%	< 5%
Annual Assessments (Updates to income, benefits, health insurance)	Evaluated for CoC-funded programs only (programs that create an APR)	% of records with overdue annual assessments (within 30 days of the Head of Household's anniversary date)	< 2%	< 2%	< 2%	< 2%	< 2%

SECTION 12.4 DATA QUALITY MANAGEMENT

Scope: Assisting CHOs in meeting requirements.
Applicability: HMIS Lead.

12.4.1 HMIS LEAD OVERSIGHT POLICY

POLICY

The HMIS Lead will work to obtain the most complete and accurate picture of homelessness within the CoC. The HMIS Lead will facilitate, support, and assist CHOs in monitoring, analyzing, and improving their data quality, and will provide regular reports to the CoC on the quality of HMIS data.

STANDARDS

» The HMIS Lead must provide regular reports to the CoC on the quality of HMIS data.

PROCEDURES

MONTHLY DATA COMPLETENESS REPORTS

1. The HMIS Lead provides monthly reports at the project level of a CoC to analyze the data entered into the HMIS that will be used for federal reporting purposes.
   a. Includes data completeness and data quality measure analysis;
   b. Intended to inform the CoC and CHOs of any data quality issues they may need to address.
   c. Publicly available via the HMIS Lead website, https://caresny.org/cchmis .
   d. It is the responsibility of the CoC and/or CHOs to check these reports, and to contact the HMIS Lead with any questions or concerns.

FINAL APR REVIEW

2. Prior to a CHO project's final APR submission in Sage, the APR is reviewed for errors by the HMIS Lead.
   a. A highlighted copy of the APR, with explanation to any notations is provided back to the CHO.

b. Intended to catch any HMIS issues or errors the CHO may need to fix with enough time to address them adequately prior to APR submission.

c. Further guidance is provided for narrative pieces, upon request.

ADDITIONAL INFORMATION

See Contracts & Agreements, Roles & Responsibilities.

12.4.2 NON-REQUIRED ORGANIZATION DATA QUALITY POLICY

POLICY

The HMIS Lead will provide select data export and data quality improvement services to homeless services organizations within the geographic area of CCHMIS-participating CoCs that are not required to participate in HMIS to obtain their data for increased HMIS coverage of CoC homeless services.

PROCEDURES

DATA EXPORTS

1. The HMIS Lead offers services for data export/import including:
   a. Assistance in formatting CSV export from software correctly for our system;
   b. Assistance in secure transmission of exports; and
   c. Review of data for data quality issues.
2. Contact the HMIS Lead Program Director for more information.

12.4.3 VENDOR CHO[10] DATA QUALITY POLICY

POLICY

As per HUD regulations, HMIS data must be collected to a central location at least once a year from all Users within the CoC. To improve data quality, the HMIS Lead will provide Vendor CHOs with select HMIS upload services to increase the frequency if HMIS data uploads, to allow for more frequent data quality analysis. The HMIS Lead will work with Vendor CHOs on data quality issues, towards the improvement of the data quality of the CoC.

PROCEDURES

MONTHLY UPLOADS

1. A Vendor CHO may provide the HMIS Lead read-only access to their HMIS to complete monthly uploads of HMIS data into the HMIS Lead HMIS database:
   a. The HMIS Lead will complete a monthly HMIS upload from the Vendor CHO database to the HMIS Lead database around the 15th of every month; and
   b. The HMIS Lead will review and assist the Vendor CHO in correcting validation errors (an HMIS Lead CSR may assist with extensive issues).
2. Vendor CHOs that do not provide the HMIS Lead access to their HMIS:
   a. The HMIS Lead will contact the Vendor CHO each month to request an upload if it has not been completed by the 15th of the month.

[10] Vendor CHO: CHOs that have independent contracts with the Continuum's selected HMIS software vendor (same software system, different data storage location) and upload their data into the HMIS regularly.

SECTION 12.5 COMPLIANCE WITH THE CCHMIS DATA QUALITY PLAN

Purpose: To ensure that all CHOs enter and maintain HMIS data at a quality level that meets or exceeds federal requirements and to ensure that all data, as much as possible, accurately represent and describe the community.
Scope: Data quality within the CoC.
Applicability: The CoC, CHOs.

12.5.1 COC DATA QUALITY POLICY

POLICY

The CoC Lead, as the official body that submits federal reports using HMIS data, is ultimately responsible for the quality of HMIS data[11], and will work with the HMIS Lead to ensure that all CHOs achieve data quality benchmarks.

STANDARDS

» The CoC Lead must ensure adequate participation in the HMIS and meet CoC benchmarks, and must intervene in any situation where they are not being met.

» The CoC Lead must work with the HMIS Lead to ensure proper compliance of Vendor CHOs, non-required organizations, and victim service providers with HMIS regulations.

12.5.2 CHO DATA QUALITY POLICY

POLICY

A CHO will follow all guidelines, standards, and requirements for HMIS data entry as set forth by HUD, the Federal Partners, and within this document To this end, a CHO will attempt, to the best of its ability, for high levels of data completeness and data quality, and will work with the HMIS to meet all Data Quality Benchmarks.

STANDARDS

» CHOs must meet or exceed all data quality benchmarks as they apply to their projects (see *Table 7*).

PROCEDURES

IMPROVING DATA QUALITY

3. The HMIS Lead provides training materials via their website to guide Users through running an HMIS Data Quality report to assess data quality at any time.
4. Upon request, the HMIS Lead will provide personal assistance to CHOs to improve data quality, including:
   a. Running reports to locate the source of issues;
   b. Training Users on how to fix errors; and
   c. Providing guidance to Users and/or administrators on how to avoid errors in the future.

***PLEASE NOTE** :Serious data quality issues requiring extensive time to rectify may incur additional service fees; see Technical Assistance.*

CONSISTENT POOR DATA QUALITY

5. See Data Quality Noncompliance Policy.

POLICY

STANDARDS

» CHOs must meet all data quality benchmarks that apply to the projects they operate within HMIS.

[11] § 580.37 Data Quality Standards and Management, HMIS Proposed Rule of 2011.

12.5.3 CHO SYSTEM SETUP DATA QUALITY POLICY

POLICY

A CHO will provide the HMIS Lead with inventory information on all projects with the HMIS to ensure system setup is correct for accurate reporting. A CHO will update the HMIS Lead regularly with any changes.

STANDARDS

» Agency must provide updated information on all HMIS projects at least once a year.

ADDITIONAL INFORMATION

The HMIS Lead requests Project Information Form verification as part of the HMIS Monitoring process.

ARTICLE 13. CCHMIS PRIVACY PLAN: CHO MINIMUM REQUIREMENTS

Purpose: The Plan described herein is intended to ensure that all organizations that process personally identifying information (PII) for the HMIS have a baseline level of privacy measures within their operations to protect client confidentiality and allow for responsible, reasonable, and limited use and disclosure of data.

Scope: All processes at CHOs involving HMIS PII.

Applicability: All CHOs (every organization that records, uses, or processes PII for an HMIS), including the HMIS Lead.

SECTION 13.1 DATA COLLECTION

13.1.1 DATA COLLECTION LIMITATION POLICY

POLICY

A CHO will collect Personally Identifying Information (PII) only when appropriate to the purposes for which the information is obtained or when required by law.

13.1.2 DATA COLLECTION STATEMENT POLICY

POLICY

A CHO will post a public sign at data collection workstations that notifies clients of HMIS PII data collection.

STANDARDS

- CHOs must ensure the sign is unobstructed and legible to clients.
- CHOs must ensure the sign, at a minimum, contains the language of the HMIS Data Collection Statement (below):

> *"We collect personal information directly from you for reasons that are discussed in our HMIS Privacy Notice. We may be required to collect some personal information by law or by organizations that give us money to operate this program. The personal information we collect is important to run our programs, to improve services for persons experiencing homelessness, and to better understand the needs of persons experiencing homelessness. We only collect information that we consider to be appropriate."*

ADDITIONAL INFORMATION

The HMIS Lead provides a compliant HMIS Data Collection Notice that CHOs may use to meet this requirement.

13.1.3 INFORMED DATA COLLECTION & CONSENT POLICY

POLICY

A CHO will collect all PII for the HMIS by lawful and fair means and, where appropriate, with the knowledge or consent of the client.

When a CHO is required by law to collect PII, it will ask for the required PII and ensure that clients understand that they may refuse to provide consent to enter their PII into the HMIS and will still be eligible to receive services.

In all circumstances, a CHO will make data collection transparent by providing clients a written copy of the CCHMIS Privacy Notice and describing the notice verbally to clients in plain language.

STANDARDS

- CHOs must allow clients to decide their consent for HMIS PII data collection and entry.
- CHOs must complete an **informed consent procedure** for every client that meets the following criteria:
    a. Is conducted **prior** to HMIS data collection and entry;

b. Provides the client with **copies** of the CCHMIS Privacy Notice and any Supplemental HMIS Privacy Notice;

c. Includes a **verbal description** of the HMIS, CCHMIS Privacy Notice, and any Supplemental HMIS Privacy Notice;

d. Provides clients an opportunity to **ask questions** regarding the HMIS and/or privacy; and

e. Obtains **written consent** via CCHMIS Inclusion Disclosure & Release of Information Form (CCHMIS ID/ROI).

- CHOs must allow clients to change their consent at any time.

ADDITIONAL INFORMATION

The HMIS Lead provides an example explanation of HMIS and the CCHMIS Privacy Notice in the Appendix.

13.1.4 RIGHT TO RECEIVE SERVICES

POLICY

A client may request an anonymous record within the HMIS, and any such request will not impact the treatment that the client will receive from the CHO and the client still has the right to receive services.

STANDARDS

- CHOs must not refuse services to a client that refuses to provide PII for the HMIS.

ADDITIONAL INFORMATION

A CHO, in recognition of the important of HMIS data, is advised to ensure any client that requests anonymization understands the importance of HMIS data collection and the protection of their data within the HMIS. See Data Quality.

13.1.5 DATA SHARING CONSENT POLICY

POLICY

A CHO will notify a client of data sharing policies and will provide the client a choice in if their data (including PII) is shared within the HMIS.

STANDARDS

- CHOs must follow all of the agency, State, and Federal rules, regulations and laws in regards to sharing client level data outside of the project.
- CHOs must use the CCHMIS Inclusion Disclosure and Release of Information Form (CCHMIS ID/ROI) for all clients at project entry, and at any time thereafter, to obtain data sharing consent within the HMIS.
- CHOs must allow clients to change their data sharing consent within the HMIS at any time.

ADDITIONAL INFORMATION

Please note*: This DOES NOT apply to Coordinated Entry processes.*

13.1.6 DATA ENTRY & ANONYMIZATION POLICY

POLICY

A CHO will enter a record into the HMIS for every client served by a project that requires HMIS data collection. A CHO will only enter PII into the record if the client provides written consent.

STANDARDS

- CHOs must enter a record into the HMIS for every client served by a project that requires HMIS data collection.
- CHOs must not enter PII into a record in the HMIS if a client does not provide consent and must instead enter non-PII into required fields, resulting in an anonymous record.

EXEMPTIONS

Victim service providers must not enter data into the HMIS, and instead must use a comparable database to record clients served.[12]

ADDITIONAL INFORMATION

The HMIS Lead provides an Anonymization Procedure for CHOs within the Appendix.

IMPORTANT: HUD regulations and notices do not specifically address the concept of entering clients as anonymous. However, since all Universal Data Elements are required for all projects, and entering clients as anonymous would circumvent this requirement, one can deduce that entering clients as anonymous does not meet the spirit of the requirement. A Continuum should do everything it can to reduce the creation of these records as they could result in duplicate records that cannot be unduplicated, thereby affect a Continuum's ability to obtain accurate counts of homeless persons and fully comply with reporting requirements.

SECTION 13.2 PURPOSE & USE LIMITATIONS

13.2.1 PURPOSE SPECIFICATION POLICY

POLICY

A CHO will specify the purposes for which it collects HMIS PII and describe all uses and disclosures of HMIS PII that may occur within a written HMIS Privacy Notice.

STANDARDS

» CHOs must ensure any that described use or disclosure does not violate any local, state, or federal laws applicable to their projects, and specify any further **limitations** on HMIS PII uses and disclosures that apply to the CHO (such as those required to meet applicable law) within a Supplemental Privacy Notice.

13.2.2 ALLOWABLE USES & DISCLOSURES POLICY

POLICY

A CHO will only use or disclose HMIS PII without consent if the use or disclosure is specified within the CCHMIS Privacy Notice, or the use or disclosure is determined by the CHO to be compatible with those specified in the Notice. No further uses or disclosures will be acceptable without additional client consent.

STANDARDS

» CHOs must ensure any that described use or disclosure does not violate any local, state, or federal laws applicable to their projects, and specify any further **limitations** on HMIS PII uses and disclosures that apply to the CHO (such as those required to meet applicable law) within a Supplemental Privacy Notice.

EXEMPTIONS

Consent for Additional Use or Disclosure Policy.

13.2.3 CONSENT FOR ADDITIONAL USE OR DISCLOSURE POLICY

POLICY

A CHO will be permitted to use or disclose HMIS PII for a purpose not specified in (nor compatible with) the allowable uses and disclosures provided within the CCHMIS Privacy Notice if they obtain prior written client consent for the use or disclosure.

STANDARDS

» Client consent for additional uses or disclosures must be provided **in writing and obtained prior** to the use or disclosure.

[12] HEARTH Act ; HMIS Proposed Rule of 2011.

SECTION 13.3 DATA QUALITY

13.3.1 DATA QUALITY REQUIREMENTS POLICY

POLICY

Data collected by a CHO will be relevant to the purpose for which it is to be used; to the extent necessary for those purposes and to the best of its ability, all collected information will be accurate, complete, and entered into the HMIS in a timely manner.

STANDARDS

- CHOs must meet the data quality requirements described within the Data Quality Plan.

13.3.2 CLIENT SELF-REPORTED DATA POLICY

POLICY

All required HMIS data will be asked of the client and responses will be recorded as the client answers them; the HMIS does not require additional paperwork/proof/documentation to enter information such as social security number, date of birth, name or disability into the HMIS. A CHO may request additional paperwork/proof/documentation if it is required by projects or public or private funders to determine eligibility for housing or services, or to assess needed services, but this does **not** apply to HMIS data entry.

STANDARDS

- CHOs must ensure that every client is asked for **ALL** required HMIS data.
- CHOs must ensure client HMIS information is collected and entered as the client provides it.

ADDITIONAL INFORMATION

See Data Quality.

13.3.3 SECURE DESTRUCTION OF DATA POLICY

POLICY

A CHO will have a secure process to destroy, or remove identifiers from, all PII collected for the HMIS if the data has not been used or updated for seven (7) years, unless a statutory, regulatory, contractual, or other requirement mandates longer retention.

STANDARDS

- CHOs must meet the secure destruction standards described within the Security Plan.
- CHOs must have data destruction processes within written policies and procedures.

SECTION 13.4 OPENNESS

13.4.1 CLIENT INQUIRIES POLICY

POLICY

A CHO will ensure that clients have an opportunity to ask questions about any HMIS information collected and privacy documents and have those questions answered.

STANDARDS

- CHOs must offer, at the time privacy documents are offered and/or presented, to explain any information within these documents that a client may not understand. (See Informed Data Collection & Consent Policy.)

13.4.2 PRIVACY NOTICE POLICY

POLICY

A CHO will have a privacy notice that fully describes its practices for the processing of HMIS PII.

STANDARDS

- » CHOs must adopt and comply with the CCHMIS Privacy Notice and have a Supplemental Privacy Notice, if necessary.

13.4.3 AMENDMENT STATEMENT POLICY

POLICY

HMIS Privacy Notices will include a statement that the notice may be amended at any time and that an amendment to the notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.

STANDARDS

- » Every HMIS Privacy Notice must have an amendment statement.

13.4.4 AVAILABILITY OF PRIVACY DOCUMENTS POLICY

POLICY

A CHO will ensure that copies of all HMIS-related privacy documents, current and historical, are available to clients.

STANDARDS

- » CHOs must publish and post a copy of the CCHMIS Privacy Notice and any Supplemental Privacy Notice to their public website, if applicable.
- » CHOs must post a sign at intake areas stating the availability of HMIS-related privacy documents.
- » CHOs must ensure that copies of the current CCHMIS Privacy Notice and any Supplemental Privacy Notice, if applicable, are available to every client at intake.
- » CHOs must provide a copy of any HMIS-related privacy document, current or historical, to any client upon request.

13.4.5 ACCOMMODATION POLICY

POLICY

A CHO that receives federal funding will provide reasonable accommodations for persons with disabilities throughout the data collection process.

STANDARDS

- » CHOs must have a process to accommodate persons with disabilities.

EXEMPTIONS

This policy does not apply to CHOs that do not receive federal financial assistance.

ADDITIONAL INFORMATION

Accommodation may include, but is not limited to, providing: information in languages other than English, 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.

SECTION 13.5 ACCESS & CORRECTION

13.5.1 ACCESS & CORRECTION POLICY

POLICY

In general, a CHO will allow a client to inspect and to have a copy of any HMIS PII about the individual and will allow a client to request correction of inaccurate or incomplete HMIS PII. A CHO is not required to remove any information from the HMIS but may, in the alternative, mark information as inaccurate or incomplete and/or may supplement it with additional information.

STANDARDS

- » CHOs must have a process to allow clients to access their own HMIS PII and to request edits to this information.
- » CHOs must offer to explain any information that a client may not understand.

ADDITIONAL INFORMATION

All requests regarding a client's HMIS record must be addressed with the CHO, as they are the responsible party for client data within the HMIS (see Data Ownership). Requests sent to the HMIS Lead will be referred to the appropriate CHO, but the HMIS Lead may assist a CHO with a client information request (see Communication).

13.5.2 DENIAL OF INFORMATION ACCESS POLICY

POLICY

A CHO may reject repeated or harassing requests for access or correction. A CHO that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the protected personal information about the individual.

STANDARDS

- » Allowable reasons for denial:
- » Information compiled in reasonable anticipation of litigation or comparable proceedings.
- » Information about another individual (other than a health care or homeless provider).
- » Information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information.
- » Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.
- » CHOs must document, in written or electronic form, any denials of information and include the reason for denial, and include this documentation in the client's records.

SECTION 13.6 ACCOUNTABILITY

13.6.1 CONFIDENTIALITY AGREEMENT POLICY

POLICY

Every individual will sign a confidentiality agreement with the CCHMIS that acknowledges receipt of a copy of the CCHMIS Privacy Notice and that pledges to comply with its requirements prior to obtaining read or write access to the HMIS. Every organization will sign a confidentiality agreement with the CCHMIS to be allowed to participate.

STANDARDS

- » All confidentiality agreements must be renewed annually.

ADDITIONAL INFORMATION

See HMIS Participation & Use Policies (CCHMIS User Agreement , CCHMIS CHO Agreement).

13.6.2 GRIEVANCE POLICY

POLICY

A CHO will have a procedure for accepting and considering questions or grievances from about its privacy and security policies and practices.

STANDARDS

- CHOs must have written policies and procedures that provide for written documentation (email or print) of client grievances and of the actions taken in response to the grievance.

SECTION 13.7 PROTECTIONS FOR VICTIMS OF DOMESTIC VIOLENCE, DATING VIOLENCE, SEXUAL ASSAULT, AND STALKING

13.7.1 VICTIM SERVICE PROVIDER POLICY

POLICY

Organizations with programs serving victims of abuse, neglect, or domestic violence will not participate in the HMIS to protect these clients whom could be physically at risk if individuals who intend to cause them harm are able to obtain personal information from the HMIS. These providers will instead enter data into a comparable database, as defined by HUD.

ADDITIONAL INFORMATION

The CoC and the HMIS Lead will work will these organizations to obtain the data necessary to produce a more complete and accurate unduplicated count of homeless individuals in the community while ensuring the protection of identifying information of clients within these programs.

SECTION 13.8 COMPLIANCE WITH CCHMIS PRIVACY PLAN

Purpose: To ensure that all organizations that process personally identifying information (PII) for the HMIS have a baseline level of privacy measures within their operations to protect client confidentiality and allow for responsible, reasonable, and limited use and disclosure of data.

Scope: All processes at CHOs involving HMIS PII, including operations at the HMIS Lead.

Applicability: All CHOs (every organization that records, uses, or processes PII for an HMIS), including the HMIS Lead.

13.8.1 MINIMUM PRIVACY REQUIREMENTS COMPLIANCE POLICY

POLICY

A CHO will comply with the minimum privacy requirements described within the CCHMIS Privacy Plan with respect to: data collection limitations; data quality; purpose and use limitations; openness; access and correction; and accountability. A CHO will comply with any additional protections described in a Supplemental HMIS Privacy Notice. Every organization with access to protected identifying information must implement procedures to ensure and monitor its compliance with applicable agreements and the requirements of this plan, including enforcement of sanctions for noncompliance.

STANDARDS

- CHOs must adopt the CCHMIS Privacy Notice, which complies with the minimum requirements for HMIS Privacy Notices herein.

- CHOs must develop procedures to meet the minimum privacy requirements described herein and in any Supplemental HMIS Privacy Notice, if applicable, including:
    a. Posted sign and availability of privacy documents;
    b. Explanation to clients of the HMIS;
    c. Description of the CCHMIS Privacy Notice; and
    d. Properly obtaining client consent.

EXEMPTIONS

See HIPAA Exemption Policy.

13.8.2 SUPPLEMENTAL HMIS PRIVACY NOTICE POLICY

POLICY

A CHO will adopt additional substantive and procedural privacy protections to comply with any federal, state and local laws that apply to the CHO and/or its projects, and may choose to adopt additional substantive and procedural privacy protections that exceed the baseline requirements described herein if these additional elements do not conflict with HMIS privacy regulations or notices and provide greater protection to clients. CHOs will describe any additional privacy protections in a Supplemental Privacy Notice that complies with all requirements herein.

STANDARDS

- CHOs must not restrict the following two mandatory HUD disclosures of HMIS information within a Supplemental Privacy Notice: first party access to information, and disclosures for oversight of compliance with HMIS privacy and security standards.
- CHOs must include an amendment statement in a Supplemental Privacy Notice.
- CHOs must retain permanent documentation of all Supplemental Privacy Notices.
- CHOs must ensure the HMIS Lead always has a current copy of a Supplemental Privacy Notice used by the CHO.

ADDITIONAL INFORMATION

See HIPAA Exemption Policy.

13.8.3 HIPAA EXEMPTION POLICY

POLICY

A CHO that determines that a substantial portion of its PII about homeless clients or homeless individuals (HMIS PII) is protected health information, as defined in the Health Insurance Portability and Accountability Act (HIPAA) standards for securing and protecting patient information rules, will not be required to follow the security and privacy standards of this document due to HIPAA regulations providing for the same or greater level of information protection compared to HMIS protections.

STANDARDS

- Any CHO with HMIS PII covered under HIPAA compliance must describe all PII the CHO collects and if it is covered under HMIS standards, HIPAA standards, no standards, or other Federal, state, or local standards in a Supplemental Privacy Notice.

13.8.4 CONSENT DOCUMENTATION POLICY

POLICY

A CHO will retain the physical documentation of each client's written consent within each client file. A CHO will be responsible for ensuring the HMIS accurately reflects the client's preferences for HMIS inclusion and HMIS data sharing from the CCHMIS Inclusion Disclosure and Release of information.

STANDARDS

- CHOs must keep physical documentation of client consent for a minimum of 7 years from the date that a client's data was last used.

ARTICLE 14. CCHMIS PRIVACY PLAN: DATA OWNERSHIP & SHARING

Purpose: To address the ownership of information within the HMIS (including transfers of ownership or responsibilities) and to provide for data sharing within the HMIS.
Scope: HMIS data, as it exists within the HMIS.
Applicability: All CHOs (every organization that records, uses, or processes PII for an HMIS), including the HMIS Lead.

SECTION 14.1 DATA OWNERSHIP

14.1.1 PRIMARY DATA OWNERSHIP POLICY

POLICY

Clients are the owner of their own data and will have the right and ability at any CHO to create, alter, share, or restrict any piece or set of data, and the ability to assign these functions and responsibilities to other parties, including the CHO.

14.1.2 TRANSFER OF DATA OWNERSHIP POLICY

POLICY

When a client seeks assistance from a CHO and consents to have their personal information entered into a record in the CCHMIS, the client assigns governance responsibility over their record within the CCHMIS to the CHO, and the CHO will be responsible for handling the records in accordance with the privacy policies and requirements herein and in any CHO-specific policies. This governance responsibility includes, as per HUD standards, that CHOs may use or disclose protected personal information (PII) from an HMIS to the HMIS Lead to carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions.

STANDARDS

- CHOs must ensure all clients are aware of this policy.

EXEMPTIONS

A CHO privacy policy that specifies data ownership and/or transfers of ownership may supersede this policy, provided the CHO properly notifies clients of the policy.

14.1.3 HMIS LEAD DATA OWNERSHIP POLICY

POLICY

The HMIS Lead does not claim any ownership of any client-level data within the HMIS.

The HMIS Lead recognizes every independent legal adult (persons over 17 years of age) as the owner of all information about themselves within the HMIS and parents, legal guardians, and/or legal power of attorneys are the designated owners of all information about household members under their guardianship, including all minors (persons under 18 years of age) and any incapacitated/disabled adults.

The HMIS Lead also recognizes a client's assignment of governance responsibility over their record to the CHO as per a signed CCHMIS Inclusion Disclosure & Release of Information, and that it is then the CHO's responsibility to update, maintain, and protect that record within the CCHMIS in accordance with all policies and requirements herein and to, generally, maintain its confidentiality.

SECTION 14.2 DATA MANAGEMENT

14.2.1 HMIS LEAD MODIFICATION OF CLIENT DATA POLICY

POLICY

The HMIS Lead will not append, edit, delete, or otherwise modify any client record within the HMIS without a written and signed request from the data owner or a direct request from an authorized member of the CHO containing the record.

STANDARDS

» Only a Agency HMIS Administrator may request modification (including removal) of more than one client record at a time.

PROCEDURES

REQUESTS TO THE HMIS LEAD TO MODIFY CLIENT DATA

Table 8. HMIS Lead modification of client records.

CLIENT	A client that wishes to have access to and/or make edits to their data must make their request to the CHO of the project containing their data of interest prior to contacting the HMIS Lead. The HMIS Lead will address client requests only after a client follows CHO procedures.
USER	Users at CHOs may submit a request to edit, amend, or delete a client's data within the HMIS via the HMIS HelpDesk.
AGENCY HMIS ADMINISTRATOR	A Agency HMIS Administrator may request changes to more than one client record at a time via a written and signed request to the HMIS Lead.

ADDITIONAL INFORMATION

Deleted or removed data cannot be recovered, and CHOs are asked to ensure that all decisions to delete data are informed and purposeful.

SECTION 14.3 DATA SHARING

CHOs and clients may decide to participate in data sharing **within the CCHMIS** with other CHOs to facilitate coordinated and more efficient service delivery for clients throughout the homeless services system.

Please note*: These policies only address data sharing within the HMIS and do NOT apply to any Coordinated Entry (CE) process or data release to external parties.*

14.3.1 GENERAL DATA SHARING POLICY

POLICY

The sharing of HMIS data among CHOs within the CoC is not required by HUD and is at the discretion of each Continuum of Care and its CHOs. HMIS data will not be shared beyond the level allowed by the most restrictive policy that applies to it.

14.3.2 PROJECT-LEVEL DATA SHARING POLICY

POLICY

The HMIS Lead will allow CHOs to determine data sharing preferences for each project within the HMIS.

STANDARDS

» CHOs must designate a level of data sharing for each project they enter data into within the HMIS.

» The HMIS Lead must ensure that HMIS settings accurately reflect the data sharing preferences of CHOs for all projects.

PROCEDURES

CHO DECISION TO DATA SHARE

1. CHOs indicate their data sharing preference for each project within their CCHMIS CHO Agreement.

14.3.3 CLIENT-LEVEL DATA SHARING POLICY

POLICY

CHOs will allow clients to determine if they want to share their data within the HMIS with other CHOs.

STANDARDS

- » Clients must indicate their preference for data sharing for each project at intake via the CCHMIS Client Inclusion Disclosure/Release of Information.
- » CHOs must ensure clients understand data sharing policies at the time of intake, including any effects that data sharing may have in how they are provided services, if any.
- » CHOs must ensure that HMIS settings reflect the data sharing preferences of clients within the HMIS.

PROCEDURES

CLIENT DECISION TO DATA SHARE

1. Clients indicate data sharing preference for a project within the CCHMIS ID/ROI form at intake.

14.3.4 DATA SHARING TRANSPARENCY POLICY

POLICY

The HMIS Lead will ensure that information regarding CHOs and projects participating in data sharing is available to CHOs and clients.

PROCEDURES

DATA SHARING RESOURCES

1. A list of CHOs and projects within the HMIS that are participating in data sharing is available via the HMIS Lead website and directly from the HMIS Lead upon request.
    a. Details regarding the level of data sharing occurring between CHOs and projects is also available from the HMIS Lead upon request.

PARTICIPATION IN DATA SHARING

2. CHOs are informed when changes are made to data sharing participation via the AWARDS Messages module.
    a. CHOs may be further informed via the CCHMIS Listserv, if appropriate.

14.3.5 COORDINATED ENTRY POLICY

POLICY

A CoC may choose to utilize HMIS functions, including data sharing options, to assist in Coordinated Entry, but the HMIS Lead will not be responsible for nor preside over any data sharing with respect to Coordinated Entry processes unless such responsibilities are written into a separate agreement.

STANDARDS

- » A CoC must have Coordinated Entry policies and procedures that address the HMIS and any HMIS data sharing within the Coordinated Entry process.
- » A CoC must create and implement a process to obtain client consent for any Coordinated Entry processes that involve the sharing of client information from a client's records.

ADDITIONAL INFORMATION

See Coordinated Entry.

ARTICLE 15. CCHMIS PRIVACY PLAN: DATA AGGREGATION & RELEASE

Purpose: To ensure safe and responsible releases of HMIS data.
Scope: HMIS data as it exists within the HMIS.
Applicability: All CHOs (every organization that records, uses, or processes PII for an HMIS) that releases HMIS data from the HMIS for any purpose, including the HMIS Lead.

SECTION 15.1 GUIDING PRINCIPLES

15.1.1 GENERAL DATA AGGREGATION

In general, as per the HMIS Proposed Rule of 2011, information in HMIS may be aggregated to:

- Obtain information about the extent and nature of homelessness over time;
- Produce an unduplicated count of homeless persons;
- Understand patterns of service use; and
- Measure the effectiveness of homeless assistance projects and programs.

Specifically, aggregate HMIS information may be used:

- By recipients and subrecipients to report to HUD and for such other reasons as may be specified in law or regulation or by HUD through notices;
- By HUD and other federal agencies to report to Congress, to evaluate recipient performance, and for such other reasons as may be specified in law or regulation or by HUD through notice; and
- For reports to the public to raise awareness and enhance local planning processes.

15.1.2 GENERAL DATA RELEASE POLICY

POLICY

Releases of aggregate HMIS data will be within the limits of and confined to that which is required by law, by the funding sources of a program, or deemed necessary by a CHO, and will be the minimum necessary to achieve the intended purpose. HMIS PII will never be distributed in aggregate unless specifically protected under an agreement with all involved parties that includes promises to maintain client confidentiality.

ADDITIONAL INFORMATION

See Research & Memorandum of Understanding (MOU) Policy.

SECTION 15.2 REPORTING

15.2.1 HMIS LEAD PUBLIC REPORTING POLICY

POLICY

The HMIS Lead will regularly provide reports to the community consisting of non-identifying, aggregate HMIS data. HMIS PII will never be distributed in a report.

STANDARDS

- All released data must be anonymous, either by removal of all identifiers and/or all information that could be used to infer an individual or household identity.
- The HMIS Lead must use data suppression techniques to prevent data disclosure.

PROCEDURES

DATA SUPPRESSION

1. See Data Suppression Policy

REQUIRED FEDERAL HMIS REPORTING

2. Continuum-wide, aggregate data will be provided to HUD annually as required.
   a. HUD reports are public information and a copy of any HUD report will be provided upon request.

NON-REQUIRED HMIS REPORTING

3. The HMIS Lead regularly reports on HMIS data at the community, CHO, and project-levels to assist in grant administration and monitoring.
   a. Community-Level: Aggregated within a Continuum of Care or a County.
   b. CHO- and Project-Level: Aggregated per CHO or per project.
4. Most CHO- and project-level reports are designed to assist in data quality improvement.
5. Reports are made publicly available on the HMIS Lead website.
6. All scheduled report release dates are approximate and are subject to change or delay at the HMIS Lead's discretion.

15.2.2 REPORT SUBMISSION POLICY

POLICY

The HMIS Lead will assist CHOs with program-level reporting to fulfill funding and grant requirements. **The HMIS Lead will NOT be responsible for submitting reports to funders on behalf of or for any CHO or program (including Federal Partners).**

STANDARDS

» CHOs must provide at least three (3) business days' notice to the HMIS Lead to compile HMIS data for a report.

PROCEDURES

REQUESTING DATA FOR A REPORT

1. Prior to a report due date, CHOs are to complete an HMIS Data Report Request Form and submit it to the HMIS Lead.
   a. Reports to request data for may include: HUD federal reports (CoC Annual Performance Reports (APR) and/or Emergency Solutions Grant (ESG) Consolidated Annual Performance and Evaluation Report (CAPER)) or Federal Partner reports (Health and Human Services, Veteran's Administration).

RESPONSE

2. The HMIS Lead will respond to the request and provide an estimated completion date.
   a. If any data cleanup is necessary, the HMIS Lead will contact the CHO with instructions and/or further information.

RHY (RUNAWAY AND HOMELESS YOUTH) REPORTING

3. The HMIS Lead provides more in-depth assistance to CHOs with RHY programs that must complete data uploads at no extra cost.

15.2.3 CHO PUBLIC REPORTING POLICY

POLICY

CHOs are responsible for handling HMIS PII in compliance with all applicable privacy policies and for preserving client confidentiality if they choose to publicly release any HMIS data.

15.2.4 DATA SUPPRESSION POLICY

POLICY

The HMIS Lead will employ data analysts to oversee the use of data suppression techniques to prevent any possible identity disclosure, attribute disclosure, or inferential disclosure from HMIS data intended for public release.

PROCEDURES

CURRENT DATA SUPPRESSION PRINCIPLES

The HMIS Lead data analysts will generally follow HIPAA principles of data suppression, and specifically employ the following:

1. Categories of data containing less than 5 individuals will not be subdivided; and
2. Categories of PII data containing less than 5 individuals will be entirely suppressed.

SECTION 15.3 HMIS COLLABORATIONS

15.3.1 RESEARCH & MEMORANDUM OF UNDERSTANDING (MOU) POLICY

POLICY

A Memorandum of Understanding (MOU) will allow disclosure of client-level HMIS PII for research purposes to a data recipient (individual or institution) if the research purpose for the MOU reflects an intent to benefit the homeless community. An MOU will ensure that the data recipient will employ privacy and security measures at least equal to those prescribed herein to ensure that the identity and confidentiality of all HMIS clients is protected and not disclosed.

See **Contracts & Agreements: Research MOU Policy** within the full CCHMIS Policies & Operations Manual for full details.

15.3.2 COORDINATED ENTRY POLICY

POLICY

The HMIS Lead will work with CoCs to utilize existing HMIS functionalities as a tool for Coordinated Entry. The HMIS Lead will **not** distribute data from the HMIS to a CoC or larger community for Coordinated Entry purposes.

STANDARDS

- A CoC must have written policies and procedures that address the use of the HMIS within the Coordinated Entry process before the HMIS Lead will assist with developing and implementing any Coordinated Entry functionalities within the HMIS.
- A CoC must create and implement a process to obtain client consent for any Coordinated Entry processes that involve any release of client information from a client's records.

PROCEDURES

ELECTRONIC WAITING LISTS (EWL)

The AWARDS Software used for the CCHMIS can create electronic waiting lists (EWL) to assist a Continuum of Care (CoC) with Coordinated Entry (CE) processes.

1. To request use of EWL for a CoC's CE process, the CoC contact for CE implementation should submit the following to the HMIS Program Director:
   a. The protocol for managing and monitoring the EWL within CE; and
   b. The consumer release that will be used with Coordinated Entry and the EWL.
2. The HMIS Program Director and HMIS System Administrator will review and work with the CoC CE contact until acceptable policies and procedures are in place to ensure the confidentiality of HMIS information within the CE process.
3. The CoC must submit a completed HMIS Use in Coordinated Entry Statement.

4. Once the Statement is received, the HMIS Lead will work to implement EWL within the HMIS for the CoC.

15.3.3 PROGRAM-SPECIFIC DATA RELEASE POLICY

POLICY

The HMIS Lead will comply with data releases required of programs funded by federal and state programs to the extent necessary to meet program requirements and limited to this extent.

PROCEDURES

STEHP SOLUTIONS TO END HOMELESSNESS PROGRAM (STEHP) DATA SHARING

1. The HMIS Lead shares aggregate data from STEHP programs within the HMIS to the New York State Office of Temporary and Disability Assistance (OTDA) to meet program reporting requirements.

OTHER PROGRAMS

2. Contact the HMIS Lead Program Director for further information on other programs that require, or have required, data release.

ARTICLE 16. CCHMIS SECURITY PLAN: ADMINISTRATIVE SAFEGUARDS

SECTION 16.1 INTRODUCTION

The HMIS Lead and HMIS Vendor share the responsibility of maintaining HMIS security – protecting the confidentiality, integrity, and availability of HMIS information while ensuring it can be used to perform its intended and permitted critical functions.

16.1.1 SECURITY PLAN ASSIGNMENT OF RESPONSIBILITY

Security of the HMIS includes the protection of **system operation and availability** as well as **the maintenance of information integrity and confidentiality**.

The former is concerned with the **(1) hardware of the system**, while the latter is concerned with: **(2) the software application, (3) the processes of accessing and using the software** to ensure only authorized use and preventing unauthorized use of information. A fourth category of security concerns **(4) the processing of HMIS data outside of the system, in any form (electronic or physical).**

(1) As the HMIS Vendor provides the physical system hardware that hosts the HMIS and stores HMIS data, the **HMIS Lead defers to the HMIS Vendor for protection of the system hardware and ensuring system availability** by contracting with the vendor for HMIS services. Relevant HMIS Vendor responsibilities include, but are not limited to: protection of the HMIS infrastructure (i.e., servers) from system crashes, including regular maintenance and infrastructure improvements as necessary; protection from malicious software attacks; maintenance of regular data backups with secured storage at a secondary location; and swift resolution of any issues that arise, despite these efforts, with a comprehensive disaster recovery plan.

(2) As the HMIS Vendor provides the software application that provides access to the HMIS, the **HMIS Lead defers to the HMIS Vendor for ensuring the software application securely accesses HMIS information** by contracting with the vendor for HMIS services. Relevant HMIS Vendor responsibilities include, but are not limited to: firewalls; encryption of data transmissions, including data entry and intra-application communication; user credentials and authentication protocols to prevent unauthorized access; encryption of stored data to protect against unauthorized access, such as hacking; complete and secure destruction of data when necessary; and regular security reviews and/or audits to ensure that security measures are updated as necessary to meet industry standards.

The **HMIS Lead has created this Security Plan** to address the responsibility for HMIS information security and confidentiality throughout the **(3) accessing and using of the software application** and the **(4) processing of HMIS information outside of the HMIS at CHOs**. This plan includes **administrative protections, access control, and minimum physical and electronic requirements for locations where HMIS PII is processed**.

16.1.2 HMIS VENDOR SECURITY POLICY

Purpose: To describe the responsibility of the HMIS Vendor for HMIS security.
Scope: HMIS hardware and software application security.
Applicability: HMIS Lead, HMIS Vendor.

POLICY

As per the HMIS Vendor contract to host and maintain the HMIS software in compliance with current HMIS security requirements as set forth by HUD, the HMIS Lead will defer to the HMIS Vendor regarding the security of the HMIS system hardware and software application.

PROCEDURES

VENDOR SECURITY

1. Per the HMIS Vendor contract, the HMIS Vendor is responsible for maintaining the security and integrity of the HMIS system and data in accordance with all federal regulations and standards.[13]
   a. Responsibilities include:
      i. User authentication;
      ii. Electronic data transmission;
      iii. Electronic data storage;
      iv. Software application back-end security measures, including:
         1. Firewalls;
         2. Encryption of data transmissions including data entry and intra-application communication;
         3. User credentials and authentication protocols to prevent unauthorized access;
         4. Encryption of stored data to protect against unauthorized access such as hacking;
         5. Complete and secure destruction of data when necessary;
         6. Protection of the HMIS infrastructure (i.e., servers) from system crashes;
         7. Protection from malicious software attacks;
         8. Maintenance of audit records for monitoring the system;
         9. Maintenance of regular data backups with secured storage at a secondary location;
         10. Regular security reviews and/or audits to ensure that security measures are updated as necessary to meet industry standards;
         11. Regular maintenance and infrastructure improvements as necessary; and
         12. Swift resolution of any issues that arise despite these efforts with a comprehensive disaster recovery plan.

COPY OF VENDOR CONTRACT

2. A copy of the HMIS Vendor contract may be obtained via a written (email or mail) request to the HMIS Program Director.

ADDITIONAL INFORMATION

More extensive security information can be found on the HMIS Vendor's website.

16.1.3 SECURITY APPLICABILITY POLICY

A CHO will implement all policies and standards to their organization as they apply to their operations and processing of HMIS information, especially PII.

STANDARDS

- » CHOs must apply the administrative security provisions to their business operations.
- » CHOs must apply system security provisions to all the systems through which HMIS PII is accessed, including, but not limited to, a CHO's networks, desktops, laptops, tablets, and any other permitted devices by the CHO.
- » CHOs must apply application security provisions to the software during HMIS data entry, storage and review or any other processing function.
- » CHOs must apply external security provisions to the locations where HMIS data is processed outside of the HMIS system. .

[13] A copy of the CARES' HMIS Vendor contract may be obtained via a written (email or mail) request to the HMIS Program Director. An overview of the HMIS Vendor's security measures is available in the appendix, and full security information can be located on their website.

SECTION 16.2 COMPLIANCE WITH SECURITY PLAN

Scope: The implementation of security measures at CHOs, including the HMIS Lead.
Applicability: All CHOs, including the HMIS Lead.

16.2.1 COMPLIANCE WITH SECURITY MEASURES POLICY

POLICY

A CHO will comply with all applicable security requirements described in this Plan and will be responsible for ensuring the compliance and proper use of the HMIS by its users. A CHO may adopt security measures in addition to the requirements herein, as long as such additional measures do not conflict with any existing policies and standards or any applicable law.

STANDARDS

- » The HMIS Lead will require CHOs to comply with the Security Plan requirements as part of the CHO HMIS Agreement.

16.2.2 SECURITY POLICIES AND PROCEDURES POLICY

POLICY

A CHO will maintain CHO-specific security policies and procedures for HMIS PII intended to maintain client confidentiality.

STANDARDS

- » CHOs must ensure their security policies and procedures are compliant with applicable federal, state, and local law.
- » CHos must ensure their security policies and procedures address on-site HMIS PII management, storage of hard-copy files, communication protocols, disposal protocols for **hard-copy and electronic** HMIS PII, and off-site and/or mobile devices HMIS access, if applicable.
- » CHOs must have all security policies and procedures in written form and available to clients upon request.

SECTION 16.3 ADMINISTRATIVE SECURITY MINIMUM REQUIREMENTS

Purpose: To ensure the security of the HMIS.
Scope: Administrative security measures for the HMIS.
Applicability: CHOs, including the HMIS Lead.

16.3.1 CHO SECURITY MANAGEMENT POLICY

POLICY

A CHO will maintain CHO-specific security policies and procedures for HMIS PII to comply with the requirements of this Plan and as necessary to meet programmatic requirements and, generally, to maintain the security and confidentiality of HMIS.

STANDARDS

- » CHOs must ensure their security policies and procedures are compliant with applicable federal, state, and local law.
- » CHOs will have policy and procedure standards establishing the technology that **protects** and **controls access** to protected electronic HMIS information, and outline the policy and procedures for its use.

- » CHOs must ensure their security policies and procedures address on-site HMIS PII management, storage of hard-copy files, communication protocols, disposal protocols for **hard-copy and electronic** HMIS PII, and off-site and/or mobile devices HMIS access, if applicable.
- » CHOs must have all security policies and procedures in written form and available to clients upon request.

ADDITIONAL INFORMATION

The HMIS Lead monitors CHOs for compliance. See HMIS Monitoring for details.

16.3.2 CHO SECURITY PERSONNEL POLICY

POLICY

A CHO will designate an Agency HMIS Administrator, who will act as the CHO-HMIS Security Officer. This HMIS Administrator will inform the CCHMIS staff of any changes in employment or access needs for designated users in compliance with the stated CCHMIS policies and procedures.

STANDARDS

- » CHOs must always have a designated HMIS Administrator and inform the HMIS Director or System administrator immediately if the person holding this position changes.
- » The Agency HMIS Administrator does not have to be an HMIS user, but rather is tasked with ensuring a smooth flow of information between the CHO and the HMIS Lead Agency

ADDITIONAL INFORMATION

The Agency HMIS Administrator, as designated within the CHO Agreement, is also the HMIS Security Officer for a CHO.

16.3.3 ACCEPTABLE USE POLICY

POLICY

A CHO will ensure that all HMIS Users follow the appropriate and acceptable conduct guidelines provided within the CCHMIS User Agreement.

16.3.4 CHO ANNUAL INTERNAL SECURITY REVIEW POLICY

POLICY

A CHO will review all internal HMIS PII processing operations at least annually to ensure the implementation of all applicable HMIS security measures and compliance with this Plan.

STANDARDS

- » Security review must occur at least annually.

16.3.5 SECURITY INCIDENT REPORTING POLICY

POLICY

A CHO will notify the HMIS Lead immediately after discovery of a security incident that involves the HMIS, where the confidentiality of HMIS PII is broken. A CHO will be responsible for notification of affected clients in the event of compromised HMIS information, if necessary.

STANDARDS

- » Reports of security incidents must be submitted by Agency HMIS Administrators to the HMIS Lead within ten (10) business days of the incident (or discovery of the incident).
- » Security incidents must be reported in writing to the HMIS Lead.

ADDITIONAL INFORMATION

The HMIS Lead provides an HMIS Security Incident Reporting form to CHOs, available on the HMIS Lead website.

SECTION 16.4 HMIS LEAD ADDITIONAL ADMINISTRATIVE SECURITY

Purpose: Administrative measures in place for or followed by the HMIS Lead to reinforce the security of the HMIS.
Scope: HMIS administrative security measures.
Applicability: HMIS Lead.

16.4.1 SECURITY PLAN MANAGEMENT POLICY

POLICY

The HMIS Lead will develop a HMIS security plan which meets the minimum requirements for a security plan as established by HUD. The HMIS Lead will review this Security Plan at least annually to ensure it remains compliant, relevant, and useful. If the Security Plan is updated, the HMIS Lead will create a plan for, and ensure, proper implementation and will provide additional guidance as necessary.

STANDARDS

- » The CoC must approve the Security Plan.
- » The HMIS Lead must review the Security Plan at least annually.
- » Full implementation of any Security Plan updates must occur within six (6) months of the effective date.

PROCEDURES

APPROVAL

1. The CoC may approve the HMIS Policies and Procedures as a whole, therefore, by default, approving the Security Plan.

REVIEW

2. A review of the Security Plan is completed at least annually by the HMIS Lead's HMIS Security Officer, consisting of:
    a. Research and review of current industry best practices;
    b. Comparison to current operations; and
    c. Recommendations for updates to current Security Plan measures, if any.
        i. The necessity of updates will be determined at the HMIS Lead's discretion Security Officer.

IMPLEMENTATION

1. If updates to the Security Plan are recommended, the HMIS Lead Security Officer:
    a. Provides a plan for proper implementation within six (6) months.
    b. Ensures notification is sent to the HMIS Security Officer at each CHO;
    c. Oversees the implementation of updated measures at the HMIS Lead; and
    d. Provides additional Information to CHOs for implementation, as requested.

FOLLOW-UP

2. Annual monitoring will include review for compliance with new measures.
3. HMIS User-related updates are included in the Annual User Review Training and the HMIS training plan is updated to reflect changes.

16.4.2 HMIS LEAD SECURITY PERSONNEL POLICY

POLICY

The HMIS Lead will designate at least one staff member as the HMIS Security Officer to develop and implement security policies and procedures and monitor for compliance with this security plan.

STANDARDS

- » The HMIS Lead must always have a designated HMIS Security Officer.
- » HMIS Security Officers must have a background check completed prior to designation.

ADDITIONAL INFORMATION/PROCEDURES

APPOINTMENT & REPLACEMENT

1. One member of the HMIS Lead will be designated the HMIS Security Officer.
2. If the current HMIS Security Officer resigns from the position or is no longer employed at the HMIS Lead, the HMIS Lead will designate another HMIS Security Officer within thirty (30) days.

ADDITIONAL INFORMATION

See the HMIS Lead website for the current HMIS Security Officer designation and contact information.

16.4.3 ADMINISTRATIVE WORKFORCE SECURITY POLICY

POLICIES

Every individual requiring administrative access to the HMIS and the HMIS Security Officer will undergo a background security screening prior to receiving administrative access to the HMIS. Only HMIS Lead staff will be eligible to receive CCHMIS Administrative access.

STANDARDS

- » Individuals must be on the HMIS Lead staff to be eligible for administrative access to the HMIS.
- » Individuals must pass the background check to be eligible for administrative access to the HMIS.

PROCEDURES

1. A background check is completed prior to administrative access being provided to an individual on the HMIS Lead staff.
    a. Only this one background check is required.

16.4.4 SECURITY AWARENESS TRAINING & FOLLOW-UP POLICY

POLICY

The HMIS Lead will ensure that all HMIS Users receive security training prior to being given access to the HMIS, and that the training reflects the policies of the Continuum of Care and the requirements of this part.

STANDARDS

- » The HMIS Lead must provide initial security training and annual security review training to all Users.
- » The HMIS Lead must ensure all Users take initial and annual security training .

ADDITIONAL INFORMATION/PROCEDURES

See Training Plan.

16.4.5 CHO ANNUAL SECURITY COMPLIANCE REVIEW POLICY

POLICY

The HMIS Lead will complete a security review of CHO operations to ensure the implementation of all applicable security measures.

STANDARDS

- » Review must occur at least annually.
- » Security review must include completion of a security checklist ensuring that each of the security standards is implemented in accordance with the HMIS security plan.

ADDITIONAL INFORMATION/PROCEDURES

Review is completed as part of the annual CHO Monitoring process. See CHO HMIS Monitoring section for details.

16.4.6 USER AUDIT REVIEW POLICY

POLICY

The HMIS Lead will monitor User audit logs within the HMIS to ensure only authorized persons are accessing the HMIS.

STANDARDS

» The HMIS Lead will review audit logs monthly and remove User access for accounts that have not been accessed for 30 days or more.

16.4.7 SECURITY AGREEMENTS POLICY

POLICY

The HMIS Lead will develop and maintain current User Access and CHO Access Agreements in compliance with HUD regulations, and will maintain document records for all active users and CHOs. Agreements will require compliance with all required security measures.

ADDITIONAL INFORMATION/PROCEDURES

See Contracts and Agreements.

16.4.8 CONTRACT & ARRANGEMENT RETENTION POLICY

POLICY

The HMIS Lead will retain copies of all contracts and arrangements executed as part of the administration and management of the HMIS. The HMIS Lead will ensure copies of are available for review.

ADDITIONAL INFORMATION/PROCEDURES

See Contracts and Agreements.

16.4.9 DISASTER RECOVERY POLICY

POLICY

The HMIS Lead will defer to the HMIS Vendor for disaster recovery, including implementation of appropriate measures to protect the system and data, creation and maintenance of system and data backups, and expedient resolution of any disaster situation while minimizing service interruption.

The HMIS Lead will be responsible for timely notification to appropriate parties regarding any disasters, including relevant updates and resolutions.

PROCEDURES

DISASTER COMMUNICATION

1. If the HMIS Lead is made aware of a disaster affecting the HMIS system and/or data by the HMIS Vendor, the HMIS Program Director will communicate the event to appropriate parties:
    a. All affected CHOs;
    b. The CCHMIS Advisory Committee; and
    c. The CoC Boards of affected communities.
2. The HMIS Program Director will instruct affected CHOs to notify affected clients, if necessary.
3. Until the situation is resolved, the HMIS Program Director will maintain contact with the HMIS Vendor and update appropriate parties (as indicated previously) with updates at least once per week.
4. The HMIS Program Director will notify appropriate parties (as indicated previously) when the situation has been resolved.

16.4.10RESPONSE TO SECURITY INCIDENTS POLICY

POLICY

The HMIS Lead will respond to all CHO reported security incidents promptly and will respond with remediation and/or disciplinary actions at the discretion of the HMIS Program Director. The HMIS Lead will maintain a record of reported security incidents.

STANDARDS

» The HMIS Lead must maintain a record of reported security incidents.

PROCEDURES

ASSESSMENT

1. If a security incident is reported to the HMIS Lead, the HMIS will review the situation, and respond with any of the following actions:
   a. If the incident involved a lost or stolen device, the HMIS Lead will reset the affected user's HMIS credentials immediately upon receiving notification, to prevent unauthorized access through the device.
   b. If the incident involved an HMIS User's deliberate actions, the HMIS Lead will deactivate the HMIS User's account.
   c. The HMIS Lead will contact the HMIS Vendor regarding the issue, if necessary.
   d. The HMIS Lead will elevate the situation to the HMIS Advisory Committee, if necessary.
      i. The HMIS Advisory Committee will be responsible for determining if client notification is necessary.

COMMUNICATION

1. The HMIS Lead will respond to the agency within two (2) business days of receiving of notification to debrief and discuss further action to take, including if client notification is required.

SECURITY INCIDENT HISTORY

2. Contact the HMIS Lead for details on reported security incidents.
   a. The CHO must contact affected clients if requested to do so by the HMIS Lead.

ARTICLE 17. CCHMIS SECURITY PLAN: PHYSICAL & TECHNICAL SAFEGUARDS

Purpose: To ensure the security of the HMIS
Scope: Physical safeguards for the HMIS. .
Applicability: CHOs, including the HMIS Lead.

SECTION 17.1 LOCATION

17.1.1 LOCATION ACCESS & CONTROL POLICY

POLICY

A CHO will limit physical access to its locations where HMIS data is processed, while ensuring that authorized access is allowed.

17.1.2 WORKSTATION SECURITY POLICY

POLICY

A CHO will ensure that all workstations where HMIS data processing is conducted meet the minimum requirements for security described below and within the Security & Privacy Checklist.

STANDARDS

- CHOS must meet the minimum requirements for workstations provided in the Security & Privacy Checklist.
- CHOs must meet the requirements below:
    a. Internet Connectivity:
        i. CHOs that connect wirelessly to the internet must use a private network (password protected) that is protected with a firewall;
        ii. CHOs that have a hardwired internet connection must have monitor the network for unauthorized connections and ensure the network is protected;
    b. Workstation – Technical:
        i. Computers must:
            1. Use Windows 7 or later;
            2. Have an active and automatically-updating antivirus software installed;
            3. Have network discovery turned off;
            4. Have a password-protected lock-out screensaver enabled that activates after 10 minutes (or less) of inactivity;
            5. Be protected with encryption upon lockout;
                a. If non-workstation devices are used to access the HMIS, devices must be protected by equivalent or greater measures as computers.
    c. Workstation – Physical:
        i. Computers must have the device viewport (screen) facing a direction that prevents viewing by unauthorized parties, including:
            1. External windows;
            2. Publicly accessible or common areas; or
            3. Security cameras.

SECTION 17.2 EXTERNAL DATA

Scope: All hard-copy information that will be entered into the HMIS, has been entered into the HMIS, or has been taken from the HMIS (including but not limited to: all data entry forms, signed client consent forms, and unreleased report data) that have been printed or written onto paper or electronic media (e.g, USB drives).
Applicability: CHOs, including the HMIS Lead.

17.2.1 HARD COPY SECURITY POLICY

POLICY

A CHO will secure any physical (paper) hard-copy HMIS data containing PII that is either generated by or for the HMIS by storing it in a locked location or supervising it at all times.

STANDARDS

- Hard-copy HMIS data must be secured in a way that prevents prevent public or unauthorized access.
- Hard-copy HMIS data must not be left unattended in any public area.

17.2.2 ELECTRONIC COPY SECURITY POLICY

POLICY

A CHO will avoid the storage of electronic (i.e., USB drives) HMIS information containing PII outside of the HMIS, if possible, and will otherwise secure and handle any of this electronic HMIS information as described here, as well as all applicable hard-copy information policies and standards.

STANDARDS

- USB drives that store any HMIS information must have lockout encryption.

17.2.3 DATA DISPOSAL POLICY

POLICY

A CHO will develop and implement a plan to dispose of or, in the alternative, to remove identifiers from, PII that is not in current use seven years after the PII was created or last changed. CHOs will include safe disposal of HMIS information containing PII outside of the HMIS in both electronic and physical forms. A CHO will be held responsible to dispose of any HMIS PII in a secure and unrecoverable way.

STANDARDS

- CHOs must have policies written and available .
- CHOs must employ physical destruction of disk drives (including USB drives) that contained PII.
- CHOs must cross-cut shred any HMIS PII in printed form.

17.2.4 HMIS USER CREDENTIAL STORAGE POLICY

POLICY

An HMIS User will not store or display electronic or hard-copy HMIS User credential information that can be used to access electronic HMIS data in a public area.

STANDARDS

- Hard-copy HMIS User credentials must be secured in a way that prevents prevent public or unauthorized access.
- Hard-copy HMIS User credentials must not be left unattended in any public area.

17.2.5 OFF-SITE & DEVICE SECURITY POLICY

POLICY

A CHO will have a policy regarding access to electronic files outside of the organization's premises, as well as accessing electronic files on devices other than workstations at the organization's premises, or will not permit these activities.

17.2.6 TRANSMISSION POLICY

POLICY

A CHO will not transmit electronic HMIS PII outside of the HMIS internal messaging system.

ARTICLE 18. CCHMIS SECURITY PLAN: ACCESS CONTROL

Purpose: To guide the management of HMIS information system accounts (User accounts) that provide access to the HMIS.

SECTION 18.1 HMIS LEAD

Scope: Management of User accounts.
Applicability: HMIS Lead.

18.1.1 USER ACCOUNT MANAGEMENT POLICY

POLICY

The HMIS Lead will create, activate, modify, deactivate, and remove information system accounts used to access to the HMIS (User accounts) as necessary to protect HMIS information availability, integrity, and confidentiality. The HMIS Lead reserves the right to restrict or deactivate User accounts at any time, without prior notice, in response to noncompliance or a security threat.

18.1.2 USER ACCOUNT PERMISSION POLICY

POLICY

The HMIS Lead will grant permissions to User accounts based on intended system usage, restricted to the minimum level necessary to perform job duties (as per the Principle of Least Privilege).

PROCEDURES

USER ACCOUNT PERMISSIONS

3. The HMIS Lead grants permissions to User accounts individually, with basic account types used as a guide (Table 9. Standard User types.*Table 9*).
   a. Standard User accounts, by default:
      i. Are prohibited from viewing or modifying records within other agencies.
      ii. Are prohibited from viewing or modifying records for non-permitted projects within their agency.
   b. Additional permissions are provided to Users as necessary (*Table 10*).

Table 9. Standard User types.

USER TYPE	EXAMPLE	DESCRIPTION OF PERMISSIONS	DETAILS
Direct Care Staff	Direct Care Staff	User can view, add, and/or modify client information for permitted projects within the CHO	Can view, add, and/or modify client information for specified projects at the CHO Perform all data entry for designated projects Use of all ReportBuilders for designated projects *Additional access to other programs within the agency and/or to fiscal/program reports with Agency HMIS Administrator approval
Read-Only User Client Level Data	Direct Care Program Director	User can only view client information (Cannot add or modify)	Use of all ReportBuilders for designated projects Ability to run different fiscal/program reports – APR, CAPER Supervisory tools to monitor their program's Users

			Access to HMIS export functionality
Read-Only User Aggregate Data	Collaborative Applicant	User can only view aggregate data (Cannot can view, add, or modify any client information)	Read-Only Access to all projects within the continuum Run all Aggregate Data ONLY reports

Table 10. Special User permissions.

PERMISSION TYPE	REQUIREMENTS	DESCRIPTION OF PERMISSIONS
Agency HMIS Administrator	Must be the designated Agency HMIS Administrator	Use of ReportBuilders for all projects within the agency, additional permissions to fiscal/program reports functions for all projects within the agency as necessary
HMIS Lead Staff Administrative User	Must be on the staff of the HMIS Lead organization Must receive a criminal background check prior	Administrative privileges for all programs and agencies within the HMIS to be able to perform the duties of the HMIS Lead Access to all HMIS data and reporting functions

18.1.3 NEW USER ACCOUNT POLICY

POLICY

The HMIS Lead will create User accounts for specific individuals at CHOs that require HMIS access to complete their job duties. The HMIS Lead will ensure that every new User account is for a current CHO employee and is for a specific individual, and that every individual receives security and privacy education and completes a CCHMIS User Agreement prior to granting a new User account.

18.1.4 DEACTIVATION/REACTIVATION OF USER ACCOUNTS POLICY

POLICY

The HMIS Lead will deactivate a User account in response to User noncompliance or a Agency HMIS Administrator request. The HMIS Lead will reactivate a User account once a User completes all requirements to be compliant with HMIS policies and procedures.

PROCEDURES

DEACTIVATION

1. The HMIS Lead deactivates a User account if **any** of the following conditions apply:
   a. The User account has not been accessed for 30 or more days;
   b. On the first business day of every month the HMIS Lead deactivates all User accounts that have not been accessed for 30 or more days;
   c. The HMIS Lead receives a request from the Agency HMIS Administrator because:
      i. The User is no longer employed by a CHO; or
      ii. The User no longer requires access to the HMIS;
   d. The User fails to complete requirements (e.g., Users that do not attend Annual Review Training and complete a new CCHMIS User Agreement before the deadline date);
   e. The User demonstrates noncompliance with HMIS policies and procedures;
   f. The User demonstrates a lack of knowledge gained from previous training; or
   g. The HMIS Lead believes the User is a credible threat to the security of the HMIS.

REACTIVATION

2. The HMIS Lead reactivates User accounts once receiving evidence that the User is back in compliance (e.g., documentation or upon training completion.)

EXEMPTIONS

The HMIS Lead System Administrator may override this policy.

SECTION 18.2 AGENCY HMIS ADMINISTRATORS

Scope: Management of organization HMIS User accounts.
Applicability: Agency HMIS Administrators.

18.2.1 ORGANIZATION MAXIMUM USER POLICY

POLICY

Agency HMIS Administrators are responsible for monitoring and ensuring that their organization does not exceed the contract limit of 15 active Users.

18.2.2 CHANGE IN EMPLOYMENT NOTIFICATION POLICY

POLICY

Agency HMIS Administrators will notify the HMIS Lead when an employee with a User account is no longer employed at the organization or an employee's responsibilities change and the employee no longer requires access to the HMIS.

PROCEDURES

EMPLOYEE STATUS CHANGE DEACTIVATION

1. A Agency HMIS Administrator MUST contact the HMIS Program Director before or within the first 24 hours of the end of a User's employment.
2. The account will be deactivated within 24 hours of notification.

SECTION 18.3 USERS

Scope: Obtaining and maintaining an active User account.
Applicability: Users.

18.3.1 NEW USER ACCOUNT REQUEST POLICY

POLICY

Data entry and editing access to the HMIS will only be available to individuals currently employed at a CHOs that have successfully completed all necessary training and signed all required documents.

STANDARDS

» Individuals must be a current CHO employee to be eligible for a new User account.
» Individuals must successfully complete New User Training to receive an active User account.
» Individuals must sign a CCHMIS User Agreement before the HMIS Lead will provide credentials for a new User account.
» An Agency HMIS Administrator or supervisor must provide written authorization for the creation of a new User account.

PROCEDURES

NEW USER ACCOUNTS

1. An individual successfully completes HMIS New User Training and signs a User Agreement.
2. The Agency HMIS Administrator makes a request to a HMIS Customer Service Representative with:
   a. The signed and dated User Agreement;
   b. A completed User Account Request form; and
   c. User training results (if completed online).

3. An HMIS Customer Service Representative will create a new User account (consisting of a unique User ID and the default Password) and provide this information to the User.
4. The User must log in to the account within 24 hours and complete a password reset.

18.3.2 USER ACCOUNT MAINTENANCE POLICY

POLICY

Individuals will comply with all applicable CHO and HMIS Lead policies and procedures to maintain User access to the HMIS database, including completion of required documents and all required and requested training sessions.

STANDARDS

- Users must comply with all HMIS Lead staff requests for User account reactivation, including additional training required for extended inactivity or a period of inactivity that included a significant system update.
- Individuals must renew their CCHMIS User Agreement annually.
- Individuals must complete annual review training on HMIS security and privacy.

PROCEDURES

ANNUAL SIGNATURE OF AGREEMENTS

1. Users must attend annual review training and sign a new CCHMIS User Agreement by the specified deadline date.
    a. Once the deadline has passed, the HMIS Lead may deactivate the User account of any noncompliant individual.

PASSWORD CHANGE/RESET

1. After contact with an HMIS Customer Service Representative informing a User that their password has been reset:
    a. The User must log into their account within 24 hours using the default password and change the default password to a new, secure password.
    b. The User must sign out and log in again with the new password to confirm the password change, or they will be locked out after 24 hours and must request a password reset again.

REACTIVATION OF INACTIVE USER ACCOUNTS

1. Users must contact an HMIS CSR after account deactivation to:
    a. Complete any requirements for account reactivation; and/or
    b. Request a password reset for reactivation.
2. Users that were inactive for an extended period (more than three (3) months without a log in attempt) will be required to go through training prior to reactivation, determined at the HMIS Lead's discretion.
3. Users must complete a password reset after account reactivation.

EXEMPTIONS

User account reactivation will occur at the HMIS Lead's discretion

ARTICLE 19. APPENDICES

SECTION 19.1 PRIVACY

19.1.1 ANONYMIZATION PROCESS FOR HMIS DATA ENTRY

ANONYMIZATION PROCESS FOR HMIS DATA ENTRY

PROCEDURE

1. A client that does not consent to HMIS PII data entry **must still** have their information collected for services as per CHO policies and procedures on **paper** forms. Best practice would be to record the unique Client ID that AWARDS assigns to the HMIS record on the paper intake form and/or folder so that agency staff can trace it back appropriately for reporting and services purposes.
2. For Coordinated Entry (CE) purposes, this anonymized record may stand in as a placeholder in the by-name list. Each CE lead must establish how the rest of the information will be communicated and whether or not the vulnerability index (minus Protected Personal Information) should be entered into the HMIS, or if the score will be entered manually by the list manager for case conferencing purposes.
3. The User entering the client's record into the HMIS must not enter personal identifiers for First Name, Last Name, Social Security Number, or Date of Birth, and instead must fill out the required UDE data elements within the record as follows (and summarized within *Table 13*):
    - a. All possible data elements must be set to "Client Refused" within the HMIS, including:
        - i. **NAME DATA QUALITY**;
        - ii. **SOCIAL SECURITY NUMBER DATA QUALITY**;
        - iii. **BIRTHDATE DATA QUALITY**;
    - b. **FIRST NAME**: Enter "Anon" into the field.
    - c. **LAST NAME**: Enter a client identifier into the field that allows the CHO to recognize the anonymous record in the system, as per the following format: *
        - i. The agency name or acronym and the 6 digit date of admission and USER initials
        - ii. Allyson Thiessen enters John Doe into CARES Housing on 1/1/20: CARES010120AT
        - iii. In the unlikely occurrence that there is more than on anonymous entry into an agency by the same user in a single day, add alphabetical identifiers; CARES010120Ata (b,c,d, etc.)
    - d. **SOCIAL SECURITY NUMBER**: Enter the number 9 for all 9 digits into the field.
    - e. **BIRTHDATE**: Enter January 1st of the client's birth year into the field.
4. Additional Household Members:
    - a. **FIRST NAME**: Enter the relationship into the field such as "Child1", "Child2", "Child3", "Partner", "Parent", "Relative".
    - b. **LAST NAME**: Use the same identifier for all household members (please see 3c above)
    - c. **SOCIAL SECURITY NUMBER**: Enter the number 9 for all 9 digits into the field.
    - d. **BIRTHDATE**: Enter January 1st of the CURRENT year into the field for minors and January 1st of the client's birth year for other adults into the field.

Table 11. Summary of data entry for a record without PII/anonymous record.

HMIS DATA FIELD	VALUE FOR USER TO ENTER	EXAMPLE
FIRST NAME	Enter "Anon"	Anon
LAST NAME	The client identifier for the client	CARES010120AT
NAME DATA QUALITY	Select "Client Refused"	

SOCIAL SECURITY NUMBER	Enter the number 9 for all 9 digits.	999-99-9999
SOCIAL SECURITY NUMBER DATA QUALITY	Select “Client Refused”	
BIRTHDATE	Enter January 1st of the year of the client’s birth	01/01/1980
BIRTHDATE DATA QUALITY	Select “Client Refused”	

19.1.2 CHO VERBAL EXPLANATION OF THE HMIS

Please verbally describe the HMIS and the terms of consent to clients at intake.

1. Explanation of HMIS:
    - a. Computer based information system that homeless services agencies across the state use to capture information about the persons they serve.
    - b. CCHMIS – the local system used at this agency.
2. Why the agency uses it:
    - a. Federal mandate that all HUD funded homeless providers must enter data into an electronic system and capture universal data elements.
    - b. Important to collect the data because the data is:
        - i. Critical to gain an accurate count of the homeless population.
        - ii. Analyzed for service use patterns to improve the success of interventions.
        - iii. Used to better understand clients’ needs.
        - iv. Used to more accurately inform public policy and the organizations that provide the funds to run this and other homeless service programs.
            1. Critical to obtain funds.
        - v. Used to plan to have appropriate resources for the people being served.
3. Security & Privacy measures:
    - a. Only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client records.
    - b. All staff must sign agreements to maintain client confidentiality, with penalties for violation.
    - c. No information will be shared to another agency without written consent.
    - d. Client has the right to not answer any question they are not comfortable with, unless entry into a program requires it.
    - e. Client information is transferred via secure connection, in an encrypted format, to the CCHMIS.
    - f. Client has the right to know who has added to, deleted, or edited their CCHMIS record and may request this information.
4. Client information in HMIS:
    - a. Client is not required to have their personally identifying information within the HMIS, but encouraged to help the program meet requirements to continue to receive its funding.
5. Data sharing:
    - a. Describe: Data sharing shares a client’s program history and personal information from a project to others within the CCHMIS
        - i. Case manager and client can use information to assist clients in obtaining resources that will help them find and keep permanent housing.
        - ii. Other agencies can see your information to streamline and future intakes, to provide more informed care decisions.

b. Inform client of the services offered on site and those offered via referral through an assessment process.
c. Inform client that this is their choice.

19.1.3 (SUGGESTED) USE OF THE HMIS IN COORDINATED ENTRY STATEMENT

To request the use of Electronic Waiting Lists, submit the following statement on company letterhead to the CCHMIS System Administrator, signed and dated by the authorized representative of the CoC:

I understand the consumer privacy implications of participating in the Electronic Waiting Lists with the ______ Continuum of Care and have a protocol in place to limit User access to projects with Waiting List level access. Additionally, I agree that all Users who will have permission to view electronic waiting lists will attend training with CARES of NY, Inc. on waiting list function, privacy and security.

Authorized CoC Representative (Signature)	Date
Authorized CoC Representative (Print Name)	Authorized CoC Representative (Title)

19.1.4 FEDERAL GUIDANCE REGARDING USES & DISCLOSURES

Direct Excerpt from The HMIS Proposed Rule of 2011 (24 CFR Parts 91, 576, 580, and 583- the Homeless Management Information Systems Requirements):

ALLOWABLE HMIS USES AND DISCLOSURES OF PROTECTED PERSONAL INFORMATION (PPI)

A CHO may use or disclose PPI from an HMIS under the following circumstances: (1) To provide or coordinate services to an individual; (2) for functions related to payment or reimbursement for services; (3) to carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; or (4) for creating de-identified PPI.

CHOs, like other institutions that maintain personal information about individuals, have obligations that may transcend the privacy interests of clients. The following additional uses and disclosures recognize those obligations to use or share personal information by balancing competing interests in a responsible and limited way. Under the HMIS privacy standard, these additional uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards). However, nothing in this standard modifies an obligation under applicable law to use or disclose personal information.

Uses and disclosures required by law. A CHO may use or disclose PPI when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law.

Uses and disclosures to avert a serious threat to health or safety. A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PPI if: (1) The CHO, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and (2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

Uses and disclosures about victims of abuse, neglect or domestic violence. A CHO may disclose PPI about an individual whom the CHO reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence under any of the following 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 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 PPI 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 beStart Printed Page 45929materially and adversely affected by waiting until the individual is able to agree to the disclosure.

A CHO that makes a permitted disclosure about victims of abuse, neglect or domestic violence must promptly inform the individual that a disclosure has been or will be made, except if:

- The CHO, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
- The CHO would be informing a personal representative (such as a family member or friend), and the CHO reasonably believes 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 determined by the CHO, in the exercise of professional judgment.

Uses and disclosures for academic research purposes. A CHO may use or disclose PPI for academic research conducted by an individual or institution that has a formal relationship with the CHO if the research is conducted either:

- By an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a program administrator (other than the individual conducting the research) designated by the CHO; or
- By an institution for use in a research project conducted under a written research agreement approved in writing by a program administrator designated by the CHO.

A written research agreement must: (1) Establish rules and limitations for the processing and security of PPI in the course of the research; (2) provide for the return or proper disposal of all PPI at the conclusion of the research; (3) restrict additional use or disclosure of PPI, except where required by law; and (4) require that the recipient of data formally agree to comply with all terms and conditions of the agreement.

A written research agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution.

Disclosures for law enforcement purposes. A CHO may, consistent with applicable law and standards of ethical conduct, disclose PPI for a law enforcement purpose to a law enforcement official under any of the following 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 protected personal information that: (1) Is signed by a supervisory official of the law enforcement agency seeking the PPI; (2) states that the information is relevant and material to a legitimate law enforcement investigation; (3) identifies the PPI sought; (4) is specific and limited in **Scope** to the extent reasonably practicable in light of the purpose for which the information is sought; and (5) states that de-identified information could not be used to accomplish the purpose of the disclosure.
- If the CHO believes in good faith that the PPI constitutes evidence of criminal conduct that occurred on the premises of the CHO;

- In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PPI disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics; or
- If (1) the official is an authorized federal official seeking PPI 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 (2) 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.

SECTION 19.2 FEES

19.2.1 EXCESS ACTIVE USER FEE POLICY

POLICY

A CHO will maintain an active User roster that does not exceed fifteen (15) Users at any given point in time. Any fees the HMIS Lead incurs from the HMIS vendor due to a CHO with excess active Users will be billed to that CHO. The HMIS Lead reserves the right to bill the CHO for administrative fees due to additional HMIS Lead staff time necessary to train and manage the HelpDesk for the increased number of Users.

STANDARDS

» CHOs must monitor their active User roster to ensure they do not exceed limits; the HMIS Lead does not monitor this.

PROCEDURES

FEES FOR EXCESS USERS

1. Fees will be billed to a CHO at the HMIS software vendor rate (See Fees within the Appendix).

Please note*: the HMIS Lead does not receive additional income from fees for excess active Users. These fees are determined by the HMIS Vendor and are passed on by the HMIS Lead with no additional charges added by the HMIS Lead.*

EXEMPTIONS

This policy does not apply to Vendor CHOs.

19.2.2 BASE TECHNICAL ASSISTANCE RATE

Current HMIS Lead base hourly rate for technical assistance: $100/hour

This rate is subject to change depending on the demands of a project.

19.2.3 EXCESS USER FEES

Cost to a CHO for excess active Users (software costs passed on directly from the Vendor):

Table 12. HMIS Vendor fees for extra Users at an agency.

TOTAL USERS	TOTAL CHO COST (PER MONTH)
16-30	$500
31-45	$1,000
46-60	$1,500
61-75	$2,000
71+	(Separate contract with vendor required)

SECTION 19.3 ADDITIONAL HMIS RESOURCES

19.3.1 LISTS

The following lists are referenced within this document and are posted on the HMIS Lead website to remain current and updated:

- CCHMIS Lead contact information
- CCHMIS Advisory Committee members
- CCHMIS Participating CHOs
  - Data sharing projects and non-data sharing projects of CHOs
- Current research collaborations with the CCHMIS
- Federal partner contact list

19.3.2 DOCUMENTS

The following independent documents are referenced by policies within this document and are posted on the HMIS Lead website:

- CCHMIS Governance Charter

CCHMIS Privacy Notice

CCHMIS CHO Agreement

CCHMIS User Agreement

19.3.3 HMIS DATA COLLECTION

The following are links to HMIS program manuals (regarding the data collection and data quality of HMIS information for these programs):

Federal Partner page: https://www.hudexchange.info/programs/hmis/federal-partner-participation/

Manual Name	Federal Partner	Program (s)
CoC Program HMIS Manual	U.S. Department of Housing and Urban Development - Office of Special Needs Assistance Programs CoC Program Information link	All Continuum of Care (CoC) Program component projects.
ESG Program HMIS Manual	U.S. Department of Housing and Urban Development - Office of Special Needs Assistance Programs ESG Program Information link	All Emergency Solution Grant (ESG) Program component projects.
HOPWA Program HMIS Manual	U.S. Department of Housing and Urban Development - Office of HIV/AIDS Housing HOPWA Program Information link	All Housing Opportunities for Persons with AIDS (HOPWA) program components.
PATH Program HMIS Manual	U.S. Department of Health and Human Services - Substance Abuse and Mental Health Services Administration PATH Program Information link	All Projects for Assistance in Transition from Homelessness (PATH) component projects.
RHY Program HMIS Manual	U.S. Department of Health and Human Services - Administration for Children and Families - Family and Youth Services Bureau RHY Program Information Link	All Runaway and Homeless Youth program component projects.
VA Program HMIS Manual	Department of Veterans Affairs VA Program information link	SSVF, GPD, and HCHV Veteran homeless programs.

VASH Program HMIS Manual	U.S. Department of Housing and Urban Development - VASH and Department of Veterans Affairs VASH Program link	Veterans Affairs Supportive Housing (VASH) program.

19.3.4 CCHMIS DATA QUALITY PLAN

INTRODUCTION

This document describes the CARES Collaborative Homeless Management System (CCHMIS) data quality plan for all the CoCs that participate in the CCHMIS. An HMIS is a locally administered electronic system that stores client level information about persons who access homeless services in a community. This document includes a Data Quality Plan and protocols for ongoing data quality monitoring that meet requirements set forth by the Department of Housing and Urban Development (HUD). It is developed by the HMIS Administrator (CARES of NY Inc), the CoCs in coordination with the CCHMIS Advisory Committee, and community service providers. This HMIS Data Quality Plan is to be updated annually, considering the latest HMIS data standards and locally developed Data Quality Thresholds.

HMIS DATA AND TECHNICAL STANDARDS

Each CoC receiving HUD funding is required to implement and participate in HMIS to capture standardized data about all persons accessing homeless assistance in the area. The HMIS complies with HUD's official data and technical standards published on HUD's Resource Exchange.

In 2010, the U.S. Interagency Council on Homelessness (USICH) affirmed HMIS as the official method of measuring outcomes for homelessness in Opening Doors: Federal Strategic Plan to Prevent and End Homelessness. Various federal partners use HMIS data for contract reporting, including:

→ U.S. Department of Housing and Urban Development (HUD)

→ U.S. Department of Health and Human Services (HHS)

→ U.S. Department of Veteran Affairs (VA)

The FY2022 Data Standards were implemented in October 2021. The standards identify Universal Data Elements and Program-Specific Data Elements that are required of all homeless programs participating in the HMIS. For further reference, please review the requirements at: FY 2022 HMIS Data Standards

What is Data Quality?

Data quality is the reliability and validity of client-level data collected. High quality data accurately reflects client information and helps case managers determine appropriate services. Data quality is measured by several factors such as timeliness, completeness, and accuracy. For System Performance Measurements, HUD's expectation is that HMIS data be complete and accurate dating back to October 1, 2012.

What is a Data Quality Plan?

A data quality plan is a community-level document that assists the CoC in achieving statistically valid and reliable data. The plan sets expectations for both the community and the end users, as well as:

→ Establishes specific data quality benchmarks for timeliness, completeness, accuracy, and consistency; Identifies the responsibilities of all parties within the CoC with respect to data quality;

→ Establishes a timeframe for monitoring data quality on a regular basis.

What is a Data Quality Monitoring Plan?

A data quality monitoring plan is a set of procedures that outlines a regular, on-going process for analyzing and reporting on the reliability and validity of the data entered into the HMIS at both the program and aggregate system levels. This plan includes roles and responsibilities for the CoC, the HMIS Administrator, and the HMIS Advisory Committee.

CCHMIS ORGANIZATIONAL CATEGORIES AND CRITERIA

	A	B	C
Funding Source	Federally funded	Not federally funded, but data is used for reporting	Not federally funded and data is not used for federal reporting
Project Participation	Participates in a HUD priority project type*	Participates in a HUD priority project type	Not participating in a HUD priority project type
Homeless Eligibility Criteria	Serves at least one of HUD's Homeless Categories**	Serves at least one of HUD's Homeless Categories	Does not need to serve HUD's Homeless Categories
Data Access	Ability to enter New Client records and Edit existing Information	Ability to enter New Client records and Edit existing Information	Ability to enter New Client records and Edit existing Information
Organizational Criteria	Mission: Serve persons experiencing homelessness or at risk of homelessness is identified as an organizational priority Services: Housing, Supportive Services, Shelter, Access to services through Coordinated Entry Service Delivery: Provide services or support for persons experiencing homelessness with the intent to improve continuity of care. Category C projects must be co-located with a homeless services provider. Email: Users must have an organizational email Security/Privacy: Organization must designate a security officer to protect client data. Data Quality: All except Category C must identify at least one individual that will respond to data quality reports sent monthly by the CCHMIS team		

* HUD's priority project types are Prevention, Street Outreach, Shelter (Emergency Shelter and/or Transitional Housing, and Housing (Rapid Re-Housing, Voucher Programs, Permanent Supportive Housing)

** HUD's four categories of homelessness are: (1) Literally Homeless (2) Imminent Risk of Homelessness (3) Homeless Under other Federal Statute (4) Fleeing/attempting to flee domestic violence.

DATA ENTRY EXPECTATIONS

UNIVERSAL DATA ELEMENTS (UDE'S)

The UDEs are baseline data collection elements required for all projects entering data into the HMIS. HMIS categories A, B, and C are required to input the following UDEs:

→ Name

→ Social Security Number

→ Date of Birth

→ Race

→ Ethnicity

→ Gender

→ Relationship to Head of Household

→ Client Location

→ Veteran Status

→ Disabling Condition

→ Project Start Date

→ Project Exit Date

→ Exit Destination

→ Prior Living Situation

→ Housing Move-In Date

→ Prior Living Situation

PROGRAM SPECIFIC ELEMENTS (PSE'S)

Program Specific Data Elements (PSEs) differ from the Universal Data Elements (UDEs) in that no one project must collect every single element in this section. Required data elements are dictated by the reporting requirements set forth by each Federal partner for the projects they fund. A Partner may require all or a selection of the fields or response categories. Data Quality Thresholds are included in Appendix C of the Data Quality Plan outlining required data elements and thresholds for each Federal partner. Category A and B projects are required to collect PDEs. HMIS PSEs include:

→ Income and Sources

→ Non-Cash Benefits

→ Health Insurance

→ Physical Disability

→ Developmental Disability

→ Chronic Health Condition

→ HIV/AIDS

→ Mental Health

→ Substance Abuse

→ Domestic Violence

→ Current living situation

→ Date of Engagement

→ Coordinated Entry Assessment

→ Coordinated Entry Event

BENCHMARKS AND GOALS

Timeliness

Timeliness refers to necessary client information being entered into HMIS within a reasonable period of time. When data is entered in a timely manner, it can reduce human error due to too much time between data collection and data entry. Relying on notes or memory of a conversation can lead to incorrect or incomplete data entry. Timely data entry also makes information more accessible for the entire CoC. All agencies can use the "HMIS Data Quality Report" in the Administration module to monitor the timeliness of data entry for entry into a project and exit from a project.

Timeliness is measured by comparing the enrollment member begin/end date to the assessment entry/exit created date. Timeliness cannot be edited, only improved going forward. Assessment information dates should match the date the client interview occurred. Each type of project has different expectations on timely data entry.

Data Entry Timeframe by Project Type

Emergency Shelter: Universal Data Elements and Housing Project Entry/Project Exit must be entered within 5 business days.

Transitional Housing: Universal Data and Program-Specific Data must be entered within 5 business days.

Permanent Housing: Universal Data and Program-Specific Data must be entered within 5 business days.

Rapid Re-Housing: Universal and Program-Specific Data Elements must be entered within 5 business days.

Prevention projects: Universal and Program-Specific Data Elements must be entered within 5 business days.

Supportive Services Only projects: Universal and Program-Specific Data Elements must be entered within 5 business days.

Outreach Projects: Limited data elements must be entered within 5 business days of the first outreach encounter. Universal Data Elements should be collected upon engagement in services.

Completeness

Completeness refers to entry of all clients served by an organization's project, as well as all necessary data elements.

Complete data is the key to assisting clients in finding the right services and benefits to end their homelessness. Incomplete data may hinder an organization's ability to provide comprehensive care to the clients it serves. Incomplete data can also negatively impact the CCHMIS's ability to make generalizations of the population each CoC serves, track patterns in client information and changes within the homeless population and adapt strategies appropriately. HMIS data quality is also part of funding applications, including CoC and ESG funding. Low HMIS data quality scores may impact and could result in denial of future funding requests.

The CCHMIS's goal is to collect 100% of all universal data elements. Therefore, the HMIS Advisory Committee has established Data Quality Thresholds (see Table 1 through 7, Appendix C). The Data Quality Thresholds set an acceptable range of "null/not collected", and "client doesn't know/client refused" responses, depending on the data element. To determine compliance, percentages will be rounded (example: .04% becomes 0%).

All programs using the HMIS shall enter data on one hundred percent (100%) of the clients they serve. It is important to note that this includes all required elements and assessments for each member of a household. These standards will be reviewed and revised annually to make sure the thresholds are reasonable.

Bed/Utilization Rates

One of the primary features of an HMIS is the ability to record the number of client stays or bed nights at a homeless residential facility. Case managers or shelter staff enter a client into the HMIS and assign them to a bed and/or a unit. The client remains there until he or she exits the program. When the client exits the project, they are also exited from the bed or unit in the HMIS. Bed/unit utilization will be determined based on project enrollment dates.

A bed night record has indicated that the client has utilized a bed in a shelter on that date

Acceptable range of bed/unit utilization rates for established projects:

→ Emergency Shelters: 85%

→ Transitional Housing: 85%

→ Permanent Supportive Housing: 85%

Each CoC recognizes that new projects may require time to reach the projected occupancy numbers and will not expect them to meet the utilization rate requirement during the first six months of operating.

Accuracy

Accuracy refers to reflecting true client information and ensuring necessary data elements are consistently recorded.

The best way to measure accuracy of client data is to compare the HMIS information with more accurate sources, such as a social security card, birth certificate, or driver's license (if available). To ensure the most up-to-date and complete data, data entry errors should be corrected monthly.

As a general rule, it is a better practice to select "client doesn't know/refused" than to misrepresent the population. Do not enter invalid data to render data completeness as this will not be counted.

Data Consistency

Consistent data collection helps promote accuracy. All data in HMIS should be collected and entered in a common and consistent manner across all programs. To that end, all intake and data entry workers will complete an initial training before accessing the live HMIS system, and access additional training opportunities offered by the HMIS Lead.

CCHMIS staff will check data accuracy and consistency by running reports that check for entry errors such as duplicate files created, overlapping enrollments or inconsistent assessment responses. The HMIS team also reserves the right to provide HMIS client identification numbers to the CoC for their program auditing or monitoring purposes.

All users are recommended to use the HMIS training projects to practice data entry or evaluate any functionality. The training projects do not affect the live database.

DATA QUALITY MONITORING PLAN

Roles and Responsibilities

For a detailed outline of the roles and responsibilities of the CoCs, HMIS Lead (CARES of NY, Inc), HMIS Advisory Committee, Data Committees, and Contributing Homeless Organizations see the "CCHMIS Administration Manual" available at caresny.org.

MONITORING WORKFLOWS

Category A Projects

HMIS Data Quality Reports

HMIS Data Quality Associate sends monthly Data Quality Reports to project's point of contact by the 5th of the month. Project's point of contact must acknowledge receipt by the 10th. Data corrections must be made by the 15th and reported to HMIS.

CCHMIS Reminder

If no response by the 15th of the month, an email reminder sent will be sent on the following business day. Project staff have 2 additional business days after this reminder to make corrections.

Data/Operations Committee Involvement

If still no response after 2 days, the CCHMIS Data Quality Associate will notify committee members at next HMIS Data/Operations Meeting, which occurs monthly. A designated committee member will reach out to the project point of contact. The CCHMIS Data Quality Associate is notified when this outreach takes place. If still no response, the information is referred to the CCHMIS Director.

Leadership Involvement

If there is still no response, the CCHMIS Director will contact the CoC Lead and the project agency's CEO/ED to evaluate the HMIS CHO Agreement.

Category B and C Projects

HMIS Data Quality Reports

HMIS Data Quality Analyst sends monthly Data Quality Reports to project's point of contact by the 5th of the month. Project's point of contact must acknowledge receipt by the 10th. Data corrections must be made by the 15th and reported to HMIS. If no response by the 15th of the month, an email reminder sent will be sent on the following business day. Project staff have 2 additional business days after this reminder to make corrections.

Data/Operations Committee Involvement

If still no response after 2 days, the CCHMIS Data Quality Associate will notify committee members at next HMIS Data/Operations Meeting, which occurs monthly. A designated committee member will reach out to the project point of contact. The CCHMIS Data Quality Associate is notified when this outreach takes place. If still no response, the information is referred to the CCHMIS Director.

Leadership Involvement

If there is still no response, the CCHMIS Director will contact the CoC Lead and the project agency's CEO/ED to evaluate the HMIS CHO Agreement.

HMIS Advisory

As Category B and C agencies do not have Federal Funding contracts, the decision at this point is whether the project should still be allowed HMIS access. This decision will be made by the HMIS Advisory Committee.