HMIS@NCCEH Operating Policies and Procedures

November 2025

TABLE OF CONTENTS

Key Terms and Acronyms 4

I. POLICIES AND PROCEDURES SUMMARY 11

A. Policy Disclaimers and Updates 11

II: Ethical Data Use 11

B. Policy Data contained in the NCCEH HMIS will only be used to support or report on the delivery of homeless and housing services in the participating CoC jurisdictions. Each HMIS End User will affirm the principles of ethical data use and client confidentiality contained in the HMIS Policies and Procedures, the HMIS Agency Participation Agreement, and the HMIS End User Agreement. These principles are: 11

C. Procedure 12

II. AGREEMENTS, CERTIFICATIONS, LICENSES AND DISCLAIMERS 13

A. HMIS Governance Charter 13

B. Project Participation: Required Agreements, Official Documents, and Policies 13

C. User Licenses and Roles in HMIS 16

D. Administrative Access 18

III. PRIVACY 20

A. Privacy and Security Plan 20

IV. DATA BACKUP AND DISASTER RECOVERY PLAN 28

A. Backup Details for the HMIS 28

B. HMIS Project Disaster Recovery Plan 28

V. SYSTEM ADMINISTRATION 29

B. Meetings in Which NCCEH System Administrators Regularly Participate 29

C. NCCEH System Administrator Responsibilities 29

VI. DATA QUALITY PLAN AND WORKFLOWS 32

D. Provider Page Set Up 32

E. Data Quality Plan 32

C. Workflow Requirements 34

VII. RESEARCH AND ELECTRONIC DATA EXCHANGES 35

F. Electronic Data Exchanges 35

APPENDIX A: HMIS Structure 37

Revision History

The HMIS Advisory Board will review these Operating Policies and Procedures on an annual basis and will approve updates as needed. Continuums of Care then review and must also approve. Suggested changes may be brought to the Advisory Board at any time via hmis@ncceh.org.

Revision Date	
June 2019	First Release
August 2020	Annual Update
August 2021	Annual Update
September 2022	Annual Update
July 2023	Annual Update
July 2024	Annual Update Clarifies HMIS is not HIPAA covered entity, updates references to federal reports, explicitly references implementation Data Quality Plan, adds a requirement for reviewing un-exited clients every 90 days.
November 2025	Annual Update Reasonable practices language added to Section 1A. Added Ethical Data Use Policy and Procedure to Section 1B and C reflecting language in the HMIS User and Ethical Standards Agreement. Added new detail to Section 3A Privacy and Security Plan on how to report Suspected PII Security Breaches (notification within 1 Business day). Updated Verbal ROI use to include Street Outreach interactions before Date of Engagement. Electronic Release of Information software specific procedure to lock down clients removed and added to internal NCCEH Standard Operating Procedure. Disclosure: Some HUD links are unavailable due to Executive Administration change and review. Many documents are expected to return in the near future.

The purpose of an HMIS project is to:

- Record and store client-level information about the characteristics and needs of persons who use homeless housing and supportive services
- Produce an unduplicated count of persons experiencing homelessness for each Continuum of Care
- Understand the extent and nature of homelessness locally, regionally, and nationally
- Understand patterns of service usage and measure the effectiveness of projects and systems of care
- Provide a platform that allows for Continuums of Care and projects to comply with HUD HMIS Data Standards, Federal reporting requirements, and other funding requirements.

These are the standards of operation for the HMIS@NCCEH. The following operating policies and procedures apply to the HMIS Lead Agency and Participating Agencies.

KEY TERMS AND ACRONYMS

Term	Acronym or another name (if used)	Brief Definition
42 CFR Part 2	**Part 2**	42 CFR Part 2 is the federal regulation governing the confidentiality of drug and alcohol use treatment and prevention records. The regulations are applicable to certain federally assisted substance use treatment programs. This law limits use and disclosure of substance use patient records and identifying information.
Administrative Use Agreement		The agreement that governs access to data for administrative use for CoC Collaborative Applicants, other funders, and contractors.
Advisory Board		Governance structure for HMIS@NCCEH. Representation by each participating CoC is maintained in the governance of HMIS. More information available on the NCCEH website.
Agency Administrator	**AA**	All Participating Agencies are required to have at least one active user with the Agency Administrator license type. Agency Administrators serve as the point of contact, provide support to Users, maintain documentation, and are responsible for privacy, security, and data quality at their Participating Agency. Appointed by agency Leadership like Executive Directors.
Agency Participation Agreement	**APA**	The agreement between NCCEH and HMIS Participating Agencies that specifies the responsibilities of Participating Agencies and allows agencies to have HMIS licenses.
By-Name List	**BNL**	A By-Name List is a list of persons experiencing homelessness within a specific jurisdiction in a defined time period. By-Name Lists can be comprehensive, meaning they include all people experiencing homelessness, or focused, meaning they contain persons with certain subpopulations, (ex. chronic or Veteran), or prioritization characteristics. By-Name Lists are frequently used within collaborative multi-partner meetings known as case conferencing sessions to link appropriate homeless persons with housing opportunities that best meet their needs.

Continuum of Care	**CoC**	Planning body charged by HUD with guiding the local response to homelessness. The CoC is responsible for designating the HMIS Lead Agency to operate the HMIS and participating in the structures (Advisory Board) to oversee effective operations of its HMIS.
Coordinated Entry	**CE** **Coordinated Assessment**	HUD requires communities to design and implement coordinated entry to be eligible to receive HUD homeless program funding. Coordinated entry systemizes access and referral to homeless resources based on a standardized assessment of need and priorities established by the community.
Covered Homeless Organizations	**CHO**	An organization that contributes data to HMIS, as defined in HUD's Data and Technical Standards for HMIS.
Conflict of Interest		Situation in which a person or organization is involved in multiple interests, financial or otherwise, where serving one interest could work against another. When conflicts of interests occur, members should disclose the conflict in writing to the HMIS@NCCEH Advisory Board Chair. The HMIS@NCCEH Advisory Board should determine the appropriate action which could be to exclude the person or organization from a conversation or vote of action.
External Visibility		Client data visibility in HMIS between different agencies and their subordinate provider pages that do not have default visibility on each other's data. This visibility in HMIS is governed by and set up according to an executed Sharing Agreement between the agencies.
Family and Youth Services Bureau	**FYSB**	A division of the U.S. Department of Health and Human Services (HHS), the Family and Youth Services Bureau provides federal resources to address homelessness among youth. FYSB oversees the Runaway and Homeless Youth Program (RHY).
Health Insurance Portability and Accountability Act of 1996	**HIPAA**	The Health Insurance Portability and Accountability Act of 1996, particularly the Privacy Rule under Title II, regulates the use and disclosure of Protected Health Information (PHI) held by covered entities and business associates. HIPAA is the foundational privacy rule on which the HMIS privacy rule is structured. *However,* HMIS Lead Agencies are not "covered entities" and not bound by HIPAA.
Homeless Definition		**See Homeless Definition Crosswalk.** **The HEARTH Act defines 4 categories of homelessness.** Not all projects can serve all categories, and some may utilize a different definition when delivering services. HMIS has adopted HUD's HEARTH Act definition for counting persons experiencing homelessness. • Category 1: Literally Homeless • Category 2: Imminent Risk of Homelessness • Category 3: Homeless under other Federal Statutes • Category 4: Fleeing/Attempting to Flee Domestic Violence (DV)
Homeless Management Information System	**HMIS**	A data system that meets HUD's HMIS requirements and is used to measure homelessness and the effectiveness of related service delivery systems. HMIS is also the primary reporting tool for HUD homeless service grants as well as for other public sources of funding related to homelessness.
HMIS@NCCEH	**HMIS**	The HMIS implementation for Durham, NC Balance of State, and Orange Continuums of Care. HMIS@NCCEH is operated by the North Carolina Coalition to End Homelessness.
HMIS Bed Coverage Rate		HMIS bed coverage rate refers to the beds dedicated to serve people experiencing homelessness that participate in HMIS. To determine bed coverage rate, the number of beds participating in the HMIS is divided by the

		total number of beds dedicated for occupancy by people experiencing homelessness in a geographic area.
HMIS Lead Agency	**HMIS Lead**	The entity which manages a CoC's Homeless Management Information System (HMIS) on behalf of the Continuum of Care. While the CoC retains ultimate authority and responsibility for a CoC's HMIS, the HMIS Lead is generally responsible for the administration, management, and operation of the HMIS implementation, in addition to providing end user training and meeting reporting requirements for funders. HUD has published an HMIS Lead Series for guidance.
HMIS Structure	**Data Tree**	HMIS is built using a database structure often referenced as a "tree." This includes an organization and all of its HMIS participating projects. A diagram of the current HMIS@NCCEH structure can be found in Appendix A. The tree is constructed of "provider pages." Each page is typically all or part of a Participating Agency's funded projects. The pages serve to associate client enrollments or services with a project or as a place holder for the organizational structure. Pages may be created for agencies not participating in HMIS to support system wide reports, such as the Housing Inventory Chart.
HMIS Software Solution Provider	**Vendor**	The HMIS Software Solution Provider is the vendor that develops, hosts, and maintains the software to HUD's specifications. HMIS@NCCEH currently utilizes Community Services software by WellSky. The HMIS Lead Agency (NCCEH) executes a contract with the HMIS Software Solution Provider on behalf of CoCs and their Participating Agencies.
HMIS User Agreement		Signed agreement governing each individual User's participation in the HMIS.
Housing Inventory Count	**HIC**	The HIC is where all residential projects (both HMIS-participating and non-participating) specify the number of beds and units available to persons experiencing homelessness within a jurisdiction. The numbers are recorded in the Participating Agency's HMIS provider pages, (for HMIS participating projects), or in "shell" provider pages (for non-participating agencies) and reported annually to HUD. The HIC is created alongside the Point-in-Time Count.
Housing Opportunities for Persons with AIDS	**HOPWA**	HOPWA is a federal program that provides housing assistance and related supportive services for persons with HIV/AIDS, and family members who are homeless or at-risk of homelessness. This project has different project reporting requirements than the other HUD-funded projects in this document.
Housing and Urban Development	**HUD**	Established as a federal department by the U.S. Housing Act of 1937, the U. S. Department of Housing and Urban Development (HUD) is f*ocused on housing and community development and dedicated to equity, inclusive communities, and quality, affordable homes for all.*
Length of Stay	**LOS**	A common variable in reports used to determine the length of time a client was served by a project. The method used to determine the LOS vary by project type. Details on methodology can be found in the HMIS Standard Reporting Terminology[Temporarily Unavailable].

Longitudinal System Analysis	**LSA**	Federally required for Continuums of Care to submit to HUD. This report includes household-level data for each fiscal year and looks back two years to compare households. Includes ES, TH, RRH, and PSH project types.
Michigan Coalition Against Homelessness	**MCAH**	The Michigan Coalition Against Homelessness is a nonprofit membership organization that is an advocate for individuals and families who are homeless or at-risk of becoming homeless, and the agencies that serve them. MCAH serves as the HMIS Lead Agency for the NC HMIS project that serves seven North Carolina Continuums of Care: • NC-500 Winston Salem/Forsyth Co. • NC-501 Asheville/Buncombe Co. • NC-504 Greensboro/High Point/Guilford Co. • NC-506 Wilmington/Brunswick/New Hanover/Pender Co. • NC-509 Gastonia/Cleveland/Gaston/Lincoln Co. • NC-511 Fayetteville/Cumberland Co. • NC-516 Northwest NC
North Carolina HMIS Governance Committee	**GC**	The NC HMIS Governance Committee is composed of representatives from the 7 North Carolina CoCs that use NC HMIS and provides direct oversight of the NC HMIS project.
North Carolina Homeless Management Information System	**NC HMIS**	The regional Homeless Management Information System(s) for 7 of North Carolina's 12 Continuums of Care. See www.nchmis.org.
NC-505 Charlotte/ Mecklenburg CoC		An independent HMIS Implementation in North Carolina.
NC-507 Raleigh/Wake CoC		An independent HMIS Implementation in North Carolina.
Participating Agency		An organization that has signed the appropriate agreements to join HMIS, has active HMIS Users, and enters client data for at least one Participating Agency project into HMIS. Participating Agencies include but are not limited to CHOs.
Personally Identifiable Information	**PII**	Personally Identifiable Information is a category of sensitive information that is associated with an individual. It should be accessed only on a strict need-to-know basis and handled and stored with care. Before any portion of the HMIS Client Record, outside of the Client Profile, can be shared, a Sharing Agreement and a client signed release of information must be in place. Defined in the 2004 Data and Technical Standards. Always PII: Name, Social Security Number, Email Address, Phone Number, Location/Physical Address Sometimes PII when combined: Date of Birth, Age, Gender, Race/Ethnicity, Client ID, Household Composition, Sexual Orientation, Project Start Date, Project Exit Date, Project Name/ID, Other Data
Privacy		**Privacy** refers to the policies and procedures that govern use and disclosure of Personally Protected Information (PPI) or Personally Identifying Information (PII) • Uses - internal activities for which providers access and interact with a person's PPI • Disclosures - the circumstances under which PPI can be shared, with or without consent

Point-in-Time Count	**PIT Count**	An annual count of people experiencing homelessness on one night, that is required of all CoCs by HUD during the last 10 days of January. As a one-night count, it is considered a minimum number of people experiencing homelessness. Additionally, communities may collect PIT counts during different times of the year. More details are available on HUD's website.
Projects for Assistance in Transition from Homelessness	**PATH**	PATH programs are funded by the Substance Abuse and Mental Health Services Administration (SAMHSA). Programs provide services to people experiencing homelessness and mental illness, primarily through street outreach, to link them to housing and services. PATH projects use HMIS to collect this information and have different reporting requirements than HUD-funded projects.
Project Types		**HUD defines 13 Project Types in HMIS:** • Coordinated Entry (CE): A CoC project that coordinates assessment and referrals of persons seeking housing and/or services and may include the use of a comprehensive and standardized assessment tool. • Day Shelter (DS): A project that provides daytime facilities and services for persons experiencing homelessness. • Emergency Shelter (ES): Overnight shelters or shelters with a planned length of stay of less than 3 months. • Transitional Housing (TH): Transitional environments with a planned LOS of not more than 2 years that provide supportive services. • PH – Housing Only: (PH): Permanent Housing that may be supported by a voucher but does not have services attached to the housing. • PH – Other Housing with Services (OPH): Permanent Housing for people with lived experience of homelessness but without disabling conditions including case management services. • PH - Permanent Supportive Housing (PSH): Permanent Housing for people with lived experience of homelessness and disabling conditions including case management services. • Rapid Re-Housing (RRH): A project that rapidly rehouses people experiencing literal homelessness. • Homeless Prevention (HP): A project that helps people who are at imminent risk of losing housing to retain their housing. • Street Outreach (SO): A project that serves persons living unsheltered who reside on the streets or other places not meant for habitation. • Supportive Services Only (SSO): A project that provides services to persons without a residential component. These projects often provide case management and other forms of support and meet with clients in an office, at the client's home, or in a shelter. • Safe Haven (SH): A project that provides low-demand shelter for hard-to-serve persons with severe disabilities. The clients have often failed in other sheltering environments. Currently, there are no funded Safe haven programs in HMIS@NCCEH. • Other: A project that cannot be categorized as any of the above options HUD defines the project descriptor data elements in the HMIS Data Standards Manual item 2.4.
Provider Page		The Provider Page is the basic organizational unit in the Community Services database. Each HMIS Participating Agency and all of its associated projects will have a separate page with administrative settings customized according to the project/Participating Agency need in the HMIS. Different levels of provider pages develop the fundamental structure of HMIS@NCCEH, CoC, Participating Agency, and Project data. Provider pages connect entries/exits,

		service transactions, and client profiles to a project for reporting purposes. Non-homeless agencies or programs can also have provider pages in HMIS, but all homeless agencies must have a provider page for the HIC.
Release of Information	**ROI**	Release of Information refers to both the electronic ROI in HMIS and paper ROI form(s). Verbal consent or a signed paper form(s) is also required for the client to authorize this visibility in HMIS and for coordination of services between agencies outside of the HMIS. An electronic ROI must be completed to indicate the client's response.
Runaway and Homeless Youth Program	**RHY**	Overseen by the Family Youth Services Bureau, the Runaway and Homeless Youth programs support street outreach, emergency shelter, transitional living, and maternity group homes for youth experiencing homelessness.
Security		Security refers to the ways in which data is protected from intentional or accidental access by unauthorized parties (or in unauthorized situations). • Unauthorized access to HMIS or client data • Improper storage of extracted HMIS data physically or digitally
Sharing		Sharing refers to the exchange of client information, including PII for data uses described in the HMIS Public Notice and/or Privacy Policy.
Sharing Agreement		The Agreement between agencies that choose to share information using the HMIS. The Agreement prevents the re-release of data, and in combination with the Participation Agreement, defines the visibility configuration of the HMIS Provider Pages.
System Administrator	**SA**	System administrators maintain the implementation of HMIS software in accordance with HUD and other funding regulations and evaluate HMIS activities. They also act as a liaison between the Continuum of Care, community partner agencies, stakeholders, and assist in the generation and submission of program and community-level data and reports from the HMIS.
System Performance Measures	**SPM**	Federally required report for Continuums of Care to submit to HUD. This report measures system outcomes and includes individual-level data for each fiscal year. Includes ES, TH, RRH, PSH, OPH, and limited SO project types.
User Agreement & Ethical Standards	**User Agreement**	The document each HMIS User signs to commit to the ethical use of HMIS and to fulfill the responsibilities as a participant in HMIS.
Visibility		Refers to whether a user granted access to one Provider Page can view client data that has been entered into another Provider Page. HMIS visibility is configured separately in each Provider Page. Visibility can be configured by individual Provider Pages and/or by Visibility Groups.
Visibility Group		A Visibility Group is a defined group of Provider Pages where data is shared. Internal Visibility Groups control internal sharing within an organization. Internal Visibility is governed by a Participating Agency's internal privacy rule. External Visibility Groups control sharing with other agencies and are defined by a Sharing Agreement.
Youth (Homeless Youth)		Homeless Youth are youth who lack a fixed, regular, or adequate nighttime residence. Depending on the program and funding source, the age and definition of youth homelessness varies. Some youth programs serve persons up to 18 years of age, while other definitions consider youth up to the age of 21 or 24. Additionally, the U.S. Department of Education considers youth that are sharing housing due to the loss of housing or economic hardship to be homeless for purposes of its programs.

I. POLICIES AND PROCEDURES SUMMARY

A. Policy Disclaimers and Updates

Operating Policies and Procedures defined in this document represent the minimum standards of participation in the HMIS project and represent general "best practice" operational procedures. Reasonable practices are HUD-mandated minimums to ensure compliance. These practices are outlined across various HUD guidance, documents, manuals, and regulations. Best practices are enhancements to HUD-mandated minimum practices that are encouraged for adoption for optimal privacy, security, and system maintenance, as resources allow. NCCEH will evaluate best practices as they become available and recommend adoption, changes to policies and procedures, and provide guidance/resources for adoption and implementation.

Operational standards in this document are not intended to supersede grant specific requirements and operating procedures as required by federal funding entities.

The HMIS Operating Policies and Procedures are updated regularly as HUD publishes additional guidance or as part of an annual review. Draft updates will be reviewed by the HMIS Advisory Board and / or Advisory Board subcommittee. Before being finalized, the HMIS Operating Policies and Procedures will be formally approved by the HMIS Advisory Board. To allow for the evolution of compliance standards without re-issuing core agreements, updated policies supersede related policies in any previously published Policies and Procedures document or agreements. Any changes from the previous year will be highlighted. A current copy of the HMIS Operating Policies and Procedures may also be found on the NCCEH website.

II: ETHICAL DATA USE

B. Policy

Data contained in the NCCEH HMIS will only be used to support or report on the delivery of homeless and housing services in the participating CoC jurisdictions. Each HMIS End User will affirm the principles of ethical data use and client confidentiality contained in the HMIS Policies and Procedures, the HMIS Agency Participation Agreement, and the HMIS End User Agreement. These principles are:

- Authorized Users will only ask Clients for information necessary to providing services, comply with contractual agreements, and to improve or better coordinate services.
- Authorized Users will ensure that Clients understand that their data is being collected and managed in the HMIS.
- Authorized Users will obtain a signed Release of Information (ROI) form before sharing client data with an outside program or agency on the HMIS.
- Authorized Users will maintain a copy of the ROI Form electronically in the client file.
- Authorized Users will not knowingly enter false and/or misleading information into the HMIS.
- Authorized Users will only use data in accordance with the CoC's Privacy Policy.

Each Authorized Agency must have a written privacy policy, including specific policies related to employee misconduct or violation of client confidentiality. All HMIS End Users are expected to understand their Agency's privacy policy.

C. Procedure

All HMIS users will sign an HMIS System End User Agreement before being given access to the HMIS. Any individual or Authorized Agency misusing or attempting to misuse NCCEH's HMIS data will be denied access to the database, and his/her relationship with the HMIS may be terminated. Any Authorized Agency for which the relationship with the HMIS is terminated may be defunded by the CoC because of the statutory requirement to participate in the Continuum's HMIS.

II. AGREEMENTS, CERTIFICATIONS, LICENSES AND DISCLAIMERS

CoCs, Agencies, and Users are required to uphold specific rules and responsibilities as participants in the HMIS.

A. HMIS Governance Charter

According to 24 CFR 578, CoCs are responsible for HMIS Governance, including (but not limited to) designating the HMIS Lead, approving policies and procedures, and monitoring. All CoCs participating in the HMIS must sign the HMIS Governance Charter that supports the ability for multiple CoCs to participate in a single HMIS. The HMIS Governance Charter established an Advisory Board to govern the HMIS project. Documents related to HMIS Governance can be found on the NCCEH website.

B. Project Participation: Required Agreements, Official Documents, and Policies

All Participating Agencies must have the following fully executed documents on file and follow the policies and directives contained therein:

1. **Agency Participation Agreement**
   Agencies providing services or housing to people experiencing homelessness may request permission to participate in HMIS and become a Participating Agency. All agencies approved to access HMIS must have a signed Agency Participation Agreement and agree to abide by the Policies and Procedures outlined in this document. The Agency Participation Agreement is a contract between the Participating Agency and NCCEH (HMIS Lead Agency). The Agency Participation Agreement outlines specific requirements on confidentiality, HMIS use, data entry, system security, and reporting. All Participating Agencies must enter client-level data into the HMIS@NCCEH implementation specified by the CoC, unless as otherwise prohibited under VAWA. Any questions regarding the terms of the Agency Participating Agreement should be submitted via hmis@ncceh.org for proper routing to NCCEH staff.
   a. Consequences for failing to meet the Agency Participation Agreement requirements may result in removal of access to HMIS and/or HMIS Lead Agency recommendation to CoCs for funding reallocation.
   b. All Participating Agencies must have at least one active user with the Agency Administrator license type.

2. **Sharing Agreements**
   The Participating Agency agrees to develop a plan for all routine sharing practices, if any, with partnering agencies and to document that plan through fully executed Sharing Agreement(s).

3. **Administrative Use Agreements** (if applicable)
   These agreements govern administrative access to the Participating Agency's data. See administrative access below.

4. **HMIS Privacy Sign (Public Notice)**
   Pursuant to the notice published by the Department of Housing and Urban Development (HUD) on July 30, 2004, the Participating Agency will prominently display at each intake desk (or comparable location) the HMIS Privacy Sign provided by NCCEH that explains generally the reasons for collecting identified information in the HMIS and the Client rights associated with providing Participating Agency staff with identified data. The Participating Agency will ensure Clients' understanding of their rights. In addition, if a Participating Agency serves Clients whose first language is not English, the Participating Agency must provide a translated version of the HMIS Privacy Sign or interpretation services. Information on HUD's four-factor analysis of reasonable language accommodations can be found in the FAQ here. The current form of the HMIS Privacy Sign, which may be modified from time to time at the HMIS Advisory Board's discretion, is available from NCCEH on its website.

5. **HMIS Privacy Notice (Privacy Policy)**
   Pursuant to the 2004 HUD HMIS Data and Technical Standards Final Notice, the Participating Agency, if it has a public website, will post the HMIS Privacy Notice on its website. In addition, the Participating Agency shall make the HMIS Privacy Notice document readily available upon Client request. In addition, if a Participating Agency serves Clients whose first language is not English, the Participating Agency must provide a translated version of the HMIS Privacy Notice or interpretation services. Information on HUD's four-factor analysis of reasonable language accommodations can be found in the FAQ here. If updated regulations are released by HUD, the Participating Agency agrees to follow the updated regulations. The current edition of the HMIS Privacy Policy document, which may be modified from time to time at the HMIS Advisory Board's discretion, is available from NCCEH on its website**.** Participating Agencies may adopt the HMIS sample notice or integrate HMIS language into their existing notice. If electing to integrate HMIS language, Participating Agencies must send a copy of the Notice to the HMIS Lead Agency for approval. All Privacy Notices must define the uses and disclosures of data collected on HMIS, including:
   a. The purposes for collection of Personally Identifying Information.
   b. A brief description of policies and procedures governing privacy, including protections for vulnerable populations.
   c. Data collection use and purpose limitations. The uses of data must specify release of aggregate, de-identified data for research or other reporting purposes. Additional disclosures may be approved by your HMIS Lead Agency upon request:
      (a) Required by Law
      (b) Serious Threat to health or safety
      (c) Abuse, Neglect, or Domestic Violence
      (d) Research
      (e) Law Enforcement: If law enforcement agencies request your information, we will immediately forward such requests to our HMIS Lead Agency (NCCEH Data Center) before taking any action.
   d. The Client's right to copy, inspect, or correct their record. Agencies may establish reasonable norms for the time and cost related to producing any copy from the record. The Participating Agency may deny a request to correct information, but the

Participating Agency must inform the Client of its reasons in writing within 60 days of the request.

e. Client Information Storage and Disposal: The Participating Agency will retain the Client record for a period of seven years. The records shall be removed and disposed of if a person or anyone in their household has not been a Client in seven years. Secure disposal must occur in a manner that ensures Client confidentiality is not compromised. Users may not store information from the system on personal portable storage devices.
f. Data Security: We implement strong technical safeguards to protect your information, including encryption, access controls, and regular security assessments. We train our staff regularly on privacy practices and limit access to only those who need it to provide services to you.
g. The Client complaint or grievance procedures, including the Security Officer's name and contact information.
h. If a Participating Agency reasonably believes that a Client is a victim of abuse, neglect, or interpersonal violence, or if a Client reports that they are a victim of abuse, neglect, or interpersonal violence, a more detailed discussion about HMIS with the Client is recommended. If entering data into HMIS poses a potential safety risk, the following protections are available to secure the record:
    a. Closing of the profile search screen so that only the Participating Agency may see the record.
    b. The right of the Client to refuse sharing, if the Participating Agency has established an external visibility plan. Client cannot be declined services based refusing external sharing/visibility.
    c. The right to be entered as an unnamed record, where identifying information is not recorded in the system, and the record is located through a randomly generated number (Note: This interface does allow for de-duplication by looking at key demographic identifiers in the system).
    d. The right to have the Client profile to be locked down in HMIS. Security of hard copy files: Agencies may create a paper record by printing the assessment screens located within HMIS. These records must be kept in accordance with the procedures that govern all hard copy information (see b. Hard copy data below).
i. Notice to the Client that the Privacy Notice may be updated over time and applies to all Client information held by the Participating Agency.
j.

6. Confidentiality Policy

A Participating Agency's board-approved Confidentiality Policy governing the privacy and security standards for the organization.

7. Grievance Policy

A Participating Agency's board-approved Grievance Policy outlining a structured process for resolving complaints or grievances against, or within, the organization.

C. User Licenses and Roles in HMIS

1. User Licenses

The following requirements below build on each other. Each consecutive role also requires the details of the previous license role.

a. **Basic HMIS User Requirements and Responsibilities**

i. A fully executed HMIS User Agreement governing the individual's participation in the system. All HMIS Users must sign and agree to and abide by the HMIS User Agreement.

ii. All Users must complete the required components of new User training, including full privacy training prior to receiving an HMIS license. The HMIS Lead Agency will determine which trainings are required based on how the User will interact with the HMIS. All Users are required to complete an updated privacy training at least annually. Participating CoCs may require additional training for their HMIS Users.

1. If CoCs have additional training requirements, they are responsible for tracking or documenting successful completion.

iii. Users are prohibited from editing their own HMIS file or files of immediate family members.

iv. Users will agree to disclose a conflict of interest to their Participating Agency Administrator.

v. If a User is suspected of violating this policy, the Participating Agency will notify NCCEH and an audit report will be run to determine if there was an infraction.

b. **Agency Administrator Requirements and Responsibilities**

In addition to the basic user license requirements above:

i. Complete all additional advanced trainings, including Reporting, as determined by the HMIS Lead Agency.

ii. Conduct regular (Monthly/ Quarterly) Data Quality monitoring and corrections.

iii. Ensure the Participating Agency's HMIS Users complete annual privacy training. Support new user during initial training period. HMIS Lead Agency Training does not replace agency-specific training needs. The Agency Administrator should treat onboarding as a hands-on mentorship period, rather than assuming that training completion alone prepares the user for success in the system.

a. During their first weeks of system use, including observing or shadowing an experienced user, receiving spot-checks on early data entry, or attending internal follow-ups with the Agency Administrator.

b. Working with user once HMIS lead had provided feedback on the user training test.

iv. Perform oversight activities defined in Privacy and Security Plan(s).

v. Attend monthly System Updates meetings.

c. **System Administrator Requirements and Responsibilities**

In addition to the above license requirements above:

i. Complete the following trainings:

a. HMIS@NCCEH Provider Page Training and Workflow Training for all workflows.
b. HMIS@NCCEH Reports Training (System Administrators are tasked with supporting data quality as well as monitoring outcomes and other performance issues).
c. System Administrator Training – This training usually takes place several weeks after a new System Administrator has been in their position.

ii. All System Administrators are required to read and understand the current version of HUD Data Standards and any updates issued by HUD to understand the rules of the HMIS and demonstrate understanding through completion of HUD's System Administration certification.

iii. Additional responsibilities of HMIS Lead Agency staff using the System Administrator license are outlined in Section V.B.

2. Project Sponsor Responsibilities

The Continuum of Care HMIS collaboration encourages service delivery partnerships between agencies and recognizes the opportunity for collaboration through shared programs and subcontracts with small service providers. However, the primary sub-recipient of all CoC funds will maintain responsibility for the collection and quality of data collected and contributed to the HMIS, either directly or indirectly. This is to ensure that sub-sub-recipients are monitored for data quality and sub-recipients have access to program data for required reporting.

a. Policy: Project Sponsors are responsible for ensuring the collection and input of required HMIS data in the HMIS. This responsibility extends to the collection and input of data acquired by any sub-recipients and contractors utilized by the project sponsor to fulfill the obligations of the grant award/contract. This responsibility must be included in all contracts and contracts must include specific conditions and procedures for acquiring, inputting, and retaining client records obtained through the program's activities.
b. Procedure: Project Sponsors must provide forms and tools to the project sponsor and sub-recipient/contractor staff that assure the correct collection and input of required project data in accordance with established data quality, data privacy, and data security policies and procedures. In the event that the project sponsor chooses to utilize a sub-recipient or contractor to fulfill its program obligations, additional required procedures are:

i. All HMIS Users, including sub-recipients and contractors of the Project Sponsor must be covered by data security liability insurance and must provide proof of adequate coverage to NCCEH as a condition of the grant award.

ii. All persons collecting or otherwise having access to the Personally Identifying Information of clients must sign an end-user agreement that binds them to HMIS policies and procedures, including data quality, privacy, and security requirements, regardless of whether a Project Sponsor or sub-recipient/contractor, and that set forth disciplinary actions for proven breaches of proper data handling.

iii. All forms of data collected, other than for the purposes of fulfilling the Project Sponsor's program requirements, must not be retained and is subject to HMIS Data Retention protocols.

c. Project Sponsors must request access to the HMIS on behalf of the sub-sub-recipient. Project Sponsors should carefully consider the extent to which a sub-sub-recipient needs access to PII and request access to the HMIS in accordance with that need.

D. Administrative Access

Administrative access may be granted to HMIS staff, funders, or contractors for administrative purposes by the HMIS Lead.

1. **System Administrators**
   a. Purpose: Designated HMIS Lead staff will be responsible for operating the HMIS.
   b. Extent: Users have full HMIS access (System Admin I or II user role in application).
   c. Limits: System Administrators ordinarily do not enter client level data in HMIS.

2. **Contractors**
   a. Purpose: NCCEH, CoC, or a Participating Agency may hire contractors to support HMIS functions.
   b. Extent: A scope of work should be defined for each contractor relationship. The User role in the HMIS will be determined based on the scope of work. The User role in the HMIS will be assigned based on a written, documented scope of work and must follow the principle of least privilege
   c. Limits: Contractors are not permitted to alter client-level data in HMIS, unless specifically defined to support a Participating Agency.
      i. (1) the work is explicitly defined in a signed contract or scope of work,
      (2) the Participating Agency and HMIS Lead have both approved access, and
      (3) the contractor has completed full privacy and security training.
      All contractor access to client-level data must be time-limited/specific and monitored."
   d. Required Documentation/ Training: Contractors will be required to sign an Administrative Use Agreement and abide by all HMIS policies and procedures. Training needs will be determined on a case-by-case basis and may include all levels of HMIS Training by NCCEH, the HMIS Software Solutions provider, or another knowledgeable entity. "All contractor access must have a set expiration date. Access must be reviewed quarterly/ (Semi) - annually by the HMIS Lead or designee, and deactivated immediately upon completion of the contract, termination of the agreement, or inactivity for more than 30 days."

3. **Funders**
   a. Purpose: Funders may want access to HMIS data to support reimbursements, contract monitoring, and/or performance reporting.
   b. Extent: Funders must notify Participating Agencies through a grant agreement or other means to inform them they require access to HMIS data before utilizing HMIS for grant

monitoring and reporting. Funders will only be provided access to their funded HMIS project(s) and will be limited to read-only user role in Community Services.

c. Limits: Funders will only be provided read-only access to the database.
d. Required documentation/ training – Funders will be required to sign an Administrative Use Agreement and abide by all HMIS policies and procedures. Training needs will be determined on a case-by-case basis and may include all levels of HMIS Training by NCCEH, the HMIS Software Solutions provider, or another knowledgeable entity. Access will not be granted until:
    a. The Participating Agency has acknowledged and confirmed the request, and
    b. The HMIS Lead has reviewed and approved the scope of access.

III. PRIVACY

A. Privacy and Security Plan

HMIS is committed to making the project safe for Participating Agencies and the Clients whose information is recorded in the system. All records entered into and downloaded from the HMIS are required to be kept in a confidential and secure manner.

1. **Oversight/Auditing**
    a. All Participating Agency Administrators with support of Participating Agency leadership must follow privacy and security procedures outlined in the HMIS@NCCEH Agency Participation Agreement and HMIS@NCCEH User Agreement and Ethical Standards. Participating Agencies are expected to conduct internal reviews of HMIS access and data entry practices at least quarterly and retain documentation of these checks for review during NCCEH audits.
    b. NCCEH will investigate a suspected breach of security or confidentiality within one business day of discovery by running applicable audit reports or notification. If NCCEH determines that a breach has occurred, and/or the staff involved violated privacy or security guidelines, the Client record(s) in question must be immediately locked down, and NCCEH will submit a written report to the HMIS Advisory Board Executive Committee within two business days. A preliminary Corrective Action Plan will be developed and implemented within five business days. Components of the plan must include, at minimum, supervision and retraining. It may also include removal of HMIS license, Client notification if a breach has occurred, and any appropriate legal action. High-risk or repeat violations, especially those involving sensitive client data, will be escalated directly to the HMIS Lead Director and may result in immediate suspension of access pending investigation
    c. NCCEH will conduct routine audits at least annually of Participating Agencies to ensure compliance with these Operating Policies and Procedures. The audit will include a mix of system reports and agency submissions. NCCEH will document the audit and any recommendations made, as well as schedule follow-up activities to identify any changes made to document compliance with these Operating Policies and Procedures. Agency audit results will be shared with their respective CoC HMIS Advisory Board representatives. Participating Agencies will be required to respond in writing within 10 business days of receiving audit results, outlining corrective actions taken or planned. NCCEH will verify completion within 30 days or escalate to the CoC HMIS Advisory Board if unresolved.
        (a) Participating Agencies must implement audit recommendations within 30 calendar days, or provide a written extension request with justification.
    d. Participating agencies agree to use HMIS as the primary system of record keeping for client documentation whenever permitted by federal, state, or funder requirements. To support compliance and streamline audit preparation, required documents—such as Release of Information forms, income and disability verification, and housing status documentation—must be uploaded into HMIS when allowable.

(1) Uploaded documents will be treated as part of the official audit documentation submission. Agencies are responsible for ensuring that documentation is:
(2) Accurate and clearly labeled
(3) Uploaded promptly,
(4) Maintained in accordance to privacy requirements
(5) While paper Copies may be kept when required, duplication is strongly discouraged when electronic storage in HMIS is sufficient.
(6) Failure to upload required documentation may result in audit findings or impact project participation in other HMIS-driven processes.

2. Participating Agency Requirements

a. Upholding Privacy Practices

Participating Agencies are required to maintain a culture that protects privacy.

(i) Staff must not discuss Personally Identifying Information in the presence of others without a need to know.
(ii) Staff must eliminate unique Personally Identifying Information before releasing data to the public.
(iii) The Participating Agency must configure workspaces for intake that support the privacy of Client interaction and data entry.
(iv) User accounts and passwords must not be shared between Users, or visible for anyone unauthorized to see. Users are prohibited from saving login information in browsers and must enter the password each time they open HMIS.
(v) Project staff must not save reports with Client identifying data on portable devices. Participating Agencies must be able to provide evidence of Users receiving training on this procedure through written training procedures or meeting minutes.
(vi) Staff must be trained regarding use of email communication, texting, file sharing, and other electronic means of transferring data related to Client services.
    1. By-Name Lists may not be printed with Personally Identifying Information without obtaining Client consent.
(v) Non-Licensed Participating Agency staff must follow all privacy procedures related to the confidentiality of HMIS Client data.
(vi) Participating Agencies are expected to conduct internal reviews of HMIS access and data entry practices at least quarterly and retain documentation of these checks for review during NCCEH audits.

b. **Privacy Policy** (HMIS Privacy Notice)

All Participating Agencies are required to have a Privacy Policy that is shared with Clients through a Privacy Notice (as detailed in section B5). Participating Agencies may elect to use the sample HMIS Privacy Notice provided by NCCEH. All Privacy Policies must include elements in the standard Privacy Notice.

1.

(ii)

c. **Privacy Script**

The Participating Agency must provide a Privacy Script to all staff charged with explaining privacy rights to Clients in order to standardize the privacy presentation. The sample Privacy Script provided by NCCEH may be used. (Participating Agencies must either adopt the sample script provided by NCCEH or develop their own Privacy Script that meets the criteria)The script must:

(i) Be developed with Participating Agency leadership to reflect the Participating Agency's Sharing Agreements and the level of risk associated with the type of data the Participating Agency collects and shares.

(ii) The script should be appropriate to the general education/literacy level of the Participating Agency's Clients, in the Client's preferred language. Information on HUD's four-factor analysis of reasonable language accommodations can be found in the FAQ here [Temporarily Unavailable]. Explain in summary what HMIS is and why agency participates. What data is collected and how it will be used.

(iii) A copy of the script should be available to Clients as they complete the intake interview.

(iv) All Participating Agency staff responsible for Client interaction must be trained in use of the script.

Privacy Script must be reviewed and updated either annually or when changes to privacy policies, sharing agreements, or HUD guidance occur. NCCEH may request to review the agency's Privacy Script and training documentation during HMIS audits or monitoring activities.

d. **Sharing Data in HMIS with Other Agencies**

Agencies that plan to share information through the HMIS must sign a Sharing Agreement that governs External Visibility Groups in HMIS.

(i) The Sharing Agreement prescribes the release of information shared between agencies under the terms of the agreement.

(ii) Participating Agencies may share different portions of a Client record with other Participating Agencies. An Agency may sign multiple Sharing Agreements to define a layered sharing practice.

(iii) Participating Agencies may share all or selected projects. If there is a project with stricter privacy laws, for example due to 42 CFR Part 2, sharing for these projects will be handled in accordance with the applicable law.

1. If a Participating Agency is a HIPAA Covered Entity, a HIPAA compliant Authorization to Release Confidential Information is also required for planned sharing or re-release of data.

(iv) The signatories of the Sharing Agreement must be representatives who have been authorized to sign such an agreement by the Participating Agency's executive leadership and/or by the Participating Agency Board of Directors.

(v) All members of a Sharing Agreement must be informed that, by sharing, they are creating a common electronic record that can impact data reflected in their reports.

(vi) HMIS licenses allow users to interact with any data they can see even if it's for another agency. Users should not modify or delete data for other agencies that they can see in the HMIS. If there are data conflicts users/agencies must agree to work together to resolve them by:

1. First negotiating and working directly with the other agency
2. Only if that is unsuccessful, escalating to the (CoC or Data Center) Staff. Data Center Staff will document the provider pages, staff, client IDs, and data elements involved internally for reference.

(vii) No Participating Agency may be added to the agreement without the approval of all other Participating Agencies.

1. Documentation of that approval must be available for review and may include such items as meeting minutes, email response, or other written documentation.
2. Participating Agency approval of additions or changes to a Sharing Agreement must be approved by a staff member with authorization to make such decisions on behalf of the Participating Agency.

(vii) When a new Participating Agency is added to the Sharing Agreement, System Administrators will determine the appropriate method to extend sharing, based on the scope and purpose of the Sharing Agreement. This may create a new Visibility Group or add a new member to an existing Visibility Group. Participating Agencies must have Client-level Release(s) of Information that are consistent with Sharing Agreements detailing the type of data the Participating Agency plans to share.

(viii) If the Participating Agency integrates the HMIS Client Release of Information into their existing releases, the release must include the following components:

1. A brief description of HMIS including a summary of the Privacy Notice including allowable uses and disclosure.
2. A specific description of the Client Profile Search Screen and an opportunity for the Client to request that the screen be closed.
3. A listing of the Participating Agency's sharing partners (if any) and a description of what is shared. These sections must reflect items negotiated in the Participating Agency's Sharing Agreement(s).
4. An expiration date of the agreement.

e. **Electronic Release of Information (ROI)**

An electronic ROI in HMIS is needed to indicate an HMIS@NCCEH Client Release of Information has been completed for each Client. Consent is given by heads of households, adults, or guardians.

(i) NCCEH System Administrators establish Internal Visibility within a Participating Agency or sharing only between a Participating Agency's provider pages by

creating visibility group(s) that include all the Participating Agency's provider pages where sharing is planned and allowed by law.

1. Internal Visibility does not require a signed HMIS ROI unless otherwise specified by law.
2. Unless otherwise specified by law, when new provider pages are added to the HMIS Data Tree, they will be included in the existing Internal Visibility group. The information available to that provider page will include all information covered by the visibility group from the beginning date of the Group – sharing will be retroactive.

(ii) Agencies may elect to share information with other agencies, a practice known as External Sharing, by negotiating a Sharing Agreement (see Section III A 2 d above).

1. External Visibility does require a signed HMIS ROI.
2. A signed and dated HMIS ROI must be stored in the Client record (paper or scanned onto the system) for all electronic ROIs that release data between different agencies.
3. NCCEH's procedure for pulling a Client's housing history across the entire database to verify a Client's eligibility for specific housing options is covered under allowable disclosures from the Privacy Notice.

(iii) Client information entered in HMIS may be used to create By-Name Lists to be used for case conferencing and prioritization meetings provided that the Client provides written consent to participate in a By-Name List and/or prioritization process. Consent for participating in this process is built into the HMIS Release of Information Section 2.

(iv) Clients who refuse consent to the external visibility should have their HMIS profile locked down according to WellSky protocols.

a.

f. **Verbal Release of Information (ROI)**

Agencies are required to have the HMIS ROI in the Client file indicating verbal consent was obtained and reviewed with the Client. Written consent must be obtained during the first in-person meeting with the Client, except for Street Outreach projects. SO projects may collect the ROI verbally up to the Date of Engagement. On the Date of Engagement, written consent (ROI) is required. If the agency only serves the Client remotely and does not meet with the Client, the Verbal ROI stands.

g. **Equal Access**

(i) The Participating Agency must have a procedure to provide privacy documents to Clients who have visual or hearing impairments or with limited English proficiency. For example:

1. Provisions for Braille or audio access
2. Availability in multiple languages
3. Availability in large print
4. Access to translation or interpretation services upon request

5. Information on HUD's four-factor analysis of reasonable language accommodations can be found in the FAQ here.

(ii) See the HUD Equal Access Rule and each CoC's Anti-Discrimination Policies for additional details related to equal access.

3. Data Security

a. HMIS Users will be issued one unique license at a time.

b. All licensed HMIS Users must be assigned Access Levels that are consistent with their job responsibilities and their business "need to know."

c. Protection of Hard Copy Data

Agencies must protect hard copy data that includes Personal Identifying Information from unauthorized viewing or access.

(i) Client files must be locked in a drawer/file cabinet.

(ii) Offices that contain Client files must be locked when not occupied.

(iii) Client files must not be left visible to unauthorized individuals.

(iv) If files are being disposed of, they should be discarded in a manner that protects Client confidentiality, e.g. shredded.

d. All computers must have network threat protection software with automatic updates.

(i) Participating Agency Administrators or designated staff are responsible for monitoring all computers that connect to the HMIS to ensure that:

1. The threat protection software is up to date.
2. That various system updates are automatic, unless a specific, documented reason exists to maintain an older version of the software.
3. Operating System updates are run regularly.

e. Physical access to computers that connect to the HMIS must be controlled.

(i) All workstations must be in secure locations (locked offices).

(ii) Workstations must be logged off when not in use.

(iii) All workstations must be password protected.

(iv) All HMIS Users are prohibited from using a computer that is available to the public.

(v) HMIS passwords are not saved in browsers.

f. Remote Access and Usage: The Participating Agency must establish a written policy that governs use of the system when access is approved from remote locations. The policy must address:

a. **Physical Location and Devices:**

i. The strict control of the use of portable storage devices with Personally Identifying Information. Data extracted from the database and stored locally must be stored in a secure location.

ii. For example, data should not be saved to DVDs/CDs or other temporary storage mechanisms like flash drives or on unprotected laptop computers.

iii. The environments where use is approved. These environments cannot be open to public access and all paper and/or electronic

records that include Personally Identifying Information must be secured in locked spaces or be password controlled.

iv. Devices must be set up in an area and at an angle so that personally identifiable data cannot be seen by unauthorized persons.

v. All devices used in a remote setting must comply with all HMIS and CoC Policies and Procedures.

vi. Shared computers should have a password protected account on the computer that is used only for work.

vii. Passwords are not to be stored in a place that is accessible by others.

viii.

b. **Wif-Fi and Software**

i. The computer must use up-to-date anti-virus software

ii. If accessing through a wireless network, that network must be encrypted and secured. All browsers used to connect to the HMIS must be secure.

iii. Do not use public Wi-Fi connections, even if they are password protected.

c. Downloading data to personal devices and storage options is not allowable. Downloads of data are only allowable to HMIS Participating Agency or HMIS Lead owned devices and storage options.

g. If staff will be using HMIS outside of the office, such as working from home, the computer and environment of data entry must meet all the standards defined above.

h. Downloads from HMIS may include Personally Identifying Information (PII), especially when used for coordination of services through the By-Name List (BNL). Data extracted from HMIS will not be transmitted outside of the private local area network unless it is properly protected via encryption or by adding a file-level Password.

i. For example, once a BNL coordination session is complete, all digital copies of PII must be deleted. All printed copies must be shredded after use.

4. **Reporting PII Security Incidents**

The HMIS Lead has created the following policy and chain of communication for reporting and responding to security incidents.

a. All HMIS users are obligated to report within 1 business day suspected instances of noncompliance with these policies and procedures that may leave HMIS data vulnerable to unauthorized access. Each HMIS Participating Agency is responsible for reporting any security incidents involving the potential or real intrusion of HMIS to NCCEH as the HMIS Lead Agency.

i. The HMIS Lead is responsible for reporting any security incidents involving potential or real intrusion of HMIS to the HMIS Advisory Board and the CoC Chairs of each participating CoC.

b. Reporting Threshold: HMIS users must report any incident in which unauthorized use or disclosure of PII has occurred. HMIS Participating Agency users will report any incident in which PII may have been used in a manner inconsistent with the HMIS Participating Agency Privacy or Security Policies. Security breaches that have the possibility to impact HMIS must be reported.

c. Reporting Procedure:

i. HMIS users will report security violations to their HMIS Participating Agency Security Officer. HMIS Participating Agency Security Officer will report violations to the HMIS Lead Security Officer.
ii. Any security breaches identified by Community Solutions/Wellsky staff will be communicated to the HMIS Lead Security Officer and System Administrators. The HMIS Lead Security Officer, in cooperation with the other HMIS Lead Agency System Administrators, will review violations and recommend corrective and disciplinary actions to the HMIS Advisory Board and the CoC Board of Directors, as appropriate. Each HMIS Participating Agency may maintain and follow procedures related to internal reporting of security incidents.

d. Audit Controls:
i. Community Solutions maintains an accessible audit trail within Community Solutions that allows the System Administrator to monitor user activity and examine data access for specific users. This Audit tool will be referenced in response to any reported security breach.
ii. NCCEH HMIS Lead System Administrators will monitor audit reports for any apparent security breaches or behavior inconsistent with the Privacy Policy outlined in these policies and procedures.

IV. DATA BACKUP AND DISASTER RECOVERY PLAN

The HMIS can be a critically important tool in the response to catastrophic events.

A. Backup Details for the HMIS

See Securing Client Data for a detailed description of data security and the Basic Disaster Response Plan from the HMIS Software Provider WellSky.

1. HMIS data is housed on a secure server by the HMIS Software Provider.
2. Back-up recovery is completed nightly off-site.
3. In case of a significant system failure at the main data center, HMIS can be brought back online within approximately four hours.
4. Validation of Off-Site storage occurs at least annually.

B. HMIS Project Disaster Recovery Plan

1. In the event of a major system failure:
   a. **If a disaster occur at WellSky, which affects the functionality and availability of Community Services, NCCEH will notify all Users and the HMIS Advisory Board. NCCEH will notify the HMIS Advisory Board of recovery activities and related timelines** as appropriate and available**.**
   b. **If a failure occurs after normal business hours, HMIS staff will report the system failure to WellSky using their emergency contact line.**
   c. NCCEH will notify WellSky if additional database services are required.

2. In the event of a local emergency, Agency Emergency Protocols should include:
   a. Emergency contact information including the names / organizations and numbers of local responders and key internal organization staff, designated representative of the CoC and the HMIS Lead Agency
   b. Persons responsible for notification and the timeline of notification to CoC and HMIS Lead Agencies

3. The System Administrator will notify WellSky Information Systems if additional database services are required.

V. SYSTEM ADMINISTRATION

The following describes the typical list of training requirements, required meetings, and responsibilities for an NCCEH System Administrator.

B. Meetings in Which NCCEH System Administrators Regularly Participate

1. Regular CoC meetings and/or workgroups as determined by the CoC.

2. The CoC Reports Committee or meetings where data use and release are discussed.

3. The HUD System Administrator calls.

4. Regular Agency Administrator/User Meetings within the CoC.

5. Calls and webinars hosted by the HMIS Software Vendor.

C. NCCEH System Administrator Responsibilities

1. Help Desk and Technical Support

a. NCCEH provides front-line technical support/technical assistance for Users and Participating Agencies. This support includes resetting passwords and troubleshooting/problem solving for Users and Agencies.
b. Where applicable, NCCEH may train Agency Administrators to do fundamental system support activities.
c. NCCEH builds relationships within the Participating Agencies they serve, working to understand the business practices of these agencies, and assisting them with mapping these business practices onto the system. NCCEH staff will be available, upon request, to provide advanced technical support.

2. User Setup

a. NCCEH staff will set up new Users in HMIS.
b. NCCEH staff will supervise license allocation for Users and Agencies. When necessary or requested, NCCEH will purchase additional licenses directly for the CoC.

3. Provider Page Setup

a. NCCEH will ensure that the Participating Agency's Provider Pages are set up correctly per HUD Data Standards.
b. NCCEH will ensure proper visibility is established for the provider pages for both Internal Visibility Groups and External Visibility Groups, per Sharing Agreements.

4. Communication

a. NCCEH will host regular User and Agency Administrator meetings for Users of the system. These meetings will cover important news on changes in the system, items of local interest within the CoC, and issues identified by NCCEH System Administrators.
b. NCCEH will share key news items of local impact, interest, or relevance to the Users and Agency Administrators in the CoC they serve.

5. Training

a. NCCEH will inform Agency Administrators and Users of required and recommended system trainings that are available remotely through the NCCEH Data Center.
b. NCCEH will provide localized training to CoC Users and Agencies for issues or items of importance related to the local community. These may include local PIT/HIC training, guidance on local data cleanup, or specific guidance on proper workflow and system usage that are identified through an audit process.
c. NCCEH will provide training for Users on initiatives identified and agreed upon between NCCEH and the local CoC.

6. HUD-Required HMIS Lead Agency Activities (Including reporting LSA, PIT/HIC, HMIS APR, SPMs, and competition HUD COC, ESG support)

a. NCCEH will work directly with CoC leadership to complete CoC-wide HUD reporting activities such as the LSA, PIT/HIC, SPMs, and the CoC HUD NOFO submission. NCCEH also assists CoCs with work surrounding state and local funding initiatives, which require data from the HMIS.
b. NCCEH will assist with completing the HMIS Annual Performance Report (APR) for the CoCs they serve, if the CoC has a HUD-funded CoC HMIS grant.
c. NCCEH System Administrators will provide support/technical assistance for Agencies completing the CoC APR and/or ESG CAPER within their jurisdiction. This includes technical assistance with data quality issues, reporting issues, etc.
    (i) This includes but is not limited to NCCEH staff participation in local CoC performance related sub-committee meetings or workgroups.
d. NCCEH will lead software evaluation efforts on behalf of participating CoCs at least annually.

7. Local CoC Reporting

a. NCCEH will be responsible for providing required HMIS reports such as:
    (i) Final reports on submissions made to HUD for various HUD-mandated activities such as the LSA, PIT/HIC, SPMs, and the HMIS APR.
    (ii) Any additional reporting requirements initiated by HUD that are required of the local CoC.
b. NCCEH will be responsible to assist the CoC to pull desired data including:
    (i) CoC-wide demographics, performance outcomes, and data quality reports that are used for informational and evaluation purposes.
    (ii) General requests for data of interest to the local CoC.

c. NCCEH will train local Agency Administrators and Users on how to run reports at the Agency level for the purpose of monitoring data quality and outcomes on a regular basis in the Participating Agency that it serves.
d. NCCEH will be responsible for generating reports on activities and expenditures to the local CoC which they serve, as directed by the CoC.

8. CoC/Participating Agency/Project Auditing and HMIS Monitoring

a. NCCEH, collaborating with Participating Agency Administrators, will audit Participating Agencies and projects to ensure compliance with HMIS requirements and HMIS@NCCEH Operating Policies and Procedures. Audit activities may include, but not be limited to:
    (i) Ensuring the Participating Agency has all required contracts, agreements, and policies in place for participation on HMIS.
    (ii) Verifying system Users have completed all required training for system participation.
    (iii) Ensuring provider pages are correctly set up per HUD Standards Guidance.
    (iv) Ensuring Agencies are following appropriate data entry protocols per the funding sources from which they receive funding.
    (v) Monitoring implementation of privacy, to ensure Client rights are being protected.
    (vi) Regularly monitoring data quality, completeness, and outcomes to ensure projects are maintaining a high level of compliance with HUD and CoC requirements.

VI. DATA QUALITY PLAN AND WORKFLOWS

D. Provider Page Set Up

1. Provider page set up is documented in the HMIS@NCCEH Configuration Standard Operating Procedures and follows HUD's Project Descriptor Data Elements standards.

E. Data Quality Plan

1. For dedicated homeless project types, agencies must require documentation at intake of the homeless status of Clients according to the reporting and eligibility guidelines issued by HUD in 24 CFR 578. The "order of priority" for obtaining evidence of homeless status are (1) third party documentation, (2) worker observations, and (3) self-certification from the person. Lack of third-party documentation may not be used to refuse emergency shelter, outreach, or domestic violence services.

2. All Participating HMIS@NCCEH Agencies must follow the CoC approved Data Quality Plan.

a. Client information should be entered into HMIS according to the Timeliness Data Standard. If the information is not entered on the same day it is collected, the Participating Agency must ensure that the date associated with the information is the date on which the data was collected by:

i. Entering data into the system using the "Enter Data As" function.
ii. Backdating the information into the system.
iii. Entering the entry/exit data as required by the project type and funding source into the system.

b. The Participating Agency must have a process to ensure the First and Last Names are spelled properly and that the Date of Birth (DOB) and at least the last four digits of the Social Security Numbers are accurate.

i. Staff should not assume they know the spelling of the name and should ask the Client for their complete spelling.
ii. No Identification card (ID) is required for HMIS data entry. Staff may use a Client's ID at intake to support accurate spelling of the Client's name, as well as the recording of the DOB. However, it should be made clear to the Client that an ID is not necessary for intake.
iii. Staff should keep in mind Equal Access Rule considerations for transgender Clients and their right to privacy and take into consideration the CoC Equal Access Policies and Procedures.
iv. Agencies may enter data for Clients with significant privacy needs under the "unnamed record" feature of the system. However, because identifiers are not stored using this feature, Users should take great care in creating the unnamed Client by carefully entering the First and Last Name and the DOB. Agencies must maintain names and HMIS Client ID number crosswalks offline in a secure location as this information will be required to find the record again.

c. Agencies must update income, non-cash benefits, and health insurance information at least annually and at exit, or at the frequency specified by program requirements.

i. For Permanent Housing Projects, the Housing Move-In Date must be completed on an Interim Update when the Client moves into housing.

ii. HMIS Annual Assessments must be completed in the 30 calendar days prior to or after the anniversary of the head of household's entry into services. (Note: This HMIS Data Standards requirement is separate from any income or eligibility verification required by certain funding sources.)

d. Participating agencies agree to use HMIS as the primary system of record keeping for client documentation whenever permitted by federal, state, or funder requirements. To support compliance and streamline audit preparation, required documents—such as Release of Information forms, income and disability verification, and housing status documentation—must be uploaded into HMIS when allowable.

Uploaded documents will be treated as part of the official audit documentation submission. Agencies are responsible for ensuring that documentation is:

- Accurate and clearly labeled
- Uploaded promptly,
- Maintained in accordance to privacy requirements

While paper Copies may be kept when required, duplication is strongly discouraged when electronic storage in HMIS is sufficient.

Failure to upload required documentation may result in audit findings or impact project participation in other HMIS-driven processes.

3. Agencies must have an organized exit process that includes:

a. Educating Clients and staff on the importance of planning and communication regarding Exit Destinations and outcomes.

b. Exit Destinations must be properly mapped to the HUD Data Standards.

(i) The NCCEH Data Center provides an Exit Destination Guide document to support proper completion of exits. All new staff must have training on this data element.

(ii) Projects must have defined processes for collecting this information from as many households as possible.

c. A procedure for communicating exit information to the person responsible for data entry, if not entering in real time.

4. Agency Administrators or staff should run data quality reports at least monthly.

a. Report frequency for all projects will also be governed by Grant Agreements, HUD reporting cycles, local CoC Written Standards, and the HMIS@NCCEH Data Quality Plan as applicable.

b. The project entry and exit dates must be recorded for all participants according to current HUD Data Standards.

c. Data quality screening and correction activities should confirm all required data is complete according to the HMIS@NCCEH Data Quality Plan, including but not limited to:

(i) Correction of missing or inaccurate information in Universal Data Element fields.

(ii) Completion of the Relationship to Household assessment questions.

(iii) Completion of the 3.917 Living Situation series of questions.
(iv) Completion of the 3.16 Enrollment CoC question.
(v) Completion of the 4.11 Domestic Violence questions.
(vi) Completion of the HUD Verifications for all Income, Non-Cash Benefits, Health Insurance, and Disability sub-assessments.
(vii) Completion of the 3.20 Housing Move-In Date for all PH projects.
(viii) Completion of all other Project Specific and Federal Partner Program Data Elements, as required by the various funding sources supporting the project.

d. Participating Agencies should review un-exited Clients in the system routinely, at least every 90 days.

5. CoCs and Agencies are required to review Outcome Performance Reports/System Performance Measures reports defined by HUD and other funding organizations. Measures are based on Project Type. The CoC Lead Agency, in collaboration with the CoC Reports Committee or other designated committee, establishes local benchmark targets for performance improvement on shared measures.

C. Workflow Requirements

1. Provider Page Configuration settings must use the assessments that are appropriate for the funding source.

2. Users responsible for data collection or entry must follow HUD, funding partner, and HMIS Lead Agency workflow guidance and Data Standards.

3. If using paper, the intake data collection forms must align correctly with HMIS Assessments. NCCEH will provide paper assessments, as appropriate.

4. 100% of Clients should be entered into HMIS with accurate and complete information no later than 6 days from the intake date.

5. Agency Administrators must actively monitor project participation and Client exits. Clients must be exited from Coordinated Entry, Night-by-Night Emergency Shelter, and Street Outreach projects within 90 days of last contact, unless project standards specify otherwise or as long as project standards do not conflict with CoC standards.

6. All required project information must be collected.

a. All Participating Agencies are required to enter the Required Data Elements for all Clients and additional data elements as approved by the HMIS Lead Agency.
b. Projects that serve Clients over time are required to complete additional updates as defined by the funding source. If the Participating Agency is not reporting to a funding source, they are required to update Client data annually by adding an interim and completing the annual assessment in HMIS.

VII. RESEARCH AND ELECTRONIC DATA EXCHANGES

F. Electronic Data Exchanges

1. **Agencies electing to import data to HMIS must coordinate with NCCEH to ensure:**
    a. Project collects all the data elements required by HUD or Federal Partner Programs.
    b. Project data adheres to the HMIS@NCCEH Data Quality Policy as approved by local CoCs.
    c. Project has staff to manage exports/imports with the appropriate HMIS license or can pay for technical services to ensure data extraction integrity, data quality control, required transformations, and periodic exports.
    d. Cost of HMIS@NCCEH (or software vendor) technical assistance and data integration services are covered by the CoC or the Participating Agency.

2. **Data Export**
    a. Agencies exporting data from HMIS must certify the privacy and security rights promised participants on HMIS are met on the destination system. If the destination system operates under less restrictive rules, the Client must be fully informed and approve the transfer during the intake process. The Participating Agency must have the ability to restrict transfers to those Clients that approve the exchange.
    b. NCCEH or the CoC may elect to participate in de-identified research data sets to support research and planning.
        (i) De-identification will involve the masking or removal of all identifying or potential identifying information such as the Name, Unique Client ID, SSN, DOB, address, agency name, and agency location.
            1. For data less one year or smaller geographic range than a CoC, suppress data at 10 people with more than one demographic stratification (race, age, gender identity, sexual orientation).
            2. Data must be CoC wide for 1 year or more to include more than one demographic stratification simultaneously.
        (ii) Geographic analysis will be restricted to prevent any data pools that are small enough to avoid inadvertently identifying a Client by other characteristics or combination of characteristics.
        (iii) Projects used to match and/or remove identifying information will not allow a re-identification process to occur. If retention of identifying information is maintained by a "trusted party" to allow for updates of an otherwise de-identified data set, the organization/person charged with retaining that data set will certify that they meet medical/behavioral health security standards and that all identifiers are kept strictly confidential and separate from the de-identified data set.

(iv) The HMIS Lead Agency will inform the HMIS Advisory Board. CoC designated representatives will provide a description of each study being implemented to their CoC membership.

c. NCCEH or the CoC may elect to participate in identified research data sets to support research and planning.
    (i) All identified research must be governed through a Data Use Agreement and aligned with Institutional Review Board approval as applicable, including requirements for Client informed consent.
    (ii) The HMIS Lead Agency will inform the HMIS Advisory Board. CoC designated representatives will provide a description of each study being implemented to their CoC membership.

APPENDIX A: HMIS STRUCTURE