San Diego County Continuum of Care
Homeless Management Information System (HMIS)

Policies and Procedures

HMIS Lead Agency
Regional Task Force on the Homeless (RTFH)

SAN DIEGO
Regional Task Force
on the Homeless

September 21, 2017

TABLE OF CONTENTS

Background

1. Project Summary

1.1 Background 3
1.2 San Diego's Continuum of Care 3
1.3 San Diego's HMIS Software 4

2. HMIS Lead Agency

2.1 Regional Task Force on the Homeless 5

3. Roles and Responsibilities

3.1 General Compliance, Documentation, and Officials 6

Monitoring and Auditing

4. Implementation

4.1 HMIS Agency Participation Agreement 15
4.2 HMIS User Agreement 15
4.3 HMIS Data Collection and Data Quality Requirements 15
4.4 Technical and Security Standards 18
4.5 Maintenance of Onsite Computer Equipment 19
4.6 HMIS Technical Support Protocol 19
4.7 System Availability 20
4.8 HMIS Participation Fees 20
4.9 Training, Ethics, and Sanctions 20

5. Privacy and Security

5.1 Privacy and Security 23
5.2 Access Controls 26
5.3 Data/Information Classification and Handling,
Collection, Maintenance, Assistance, and System Availability 27
5.4 Privacy Use and Disclosures 29

Appendices

Appendix A: Agency Participation Agreement
Appendix B: HMIS User Agreement
Appendix C: Multiparty Authorization to Use and/or Disclose Information
Appendix D: Notice of Privacy Practices
Appendix E: Summary of Privacy Practices
Appendix F: Mandatory Collection Notice
Appendix G: Client Revocation of Authorization to Use and/or Disclose Information
Appendix H: Grievance Procedure
Appendix I: Policies and Procedures Legal Framework
Appendix J: Policies and Procedures Revision History
Appendix K: Glossary

1. PROJECT SUMMARY

1.1 Background

To end homelessness, a community must know the scope of the problem, the characteristics of those who find themselves homeless, and understand what is working in their community and what is not. Solid data enables a community to work confidently towards their goals as they measure outputs, outcomes, and impacts.

A Homeless Management Information System (HMIS) is the information system designated by a local Continuum of Care (CoC) to comply with the requirements of CoC Program interim rule 24 CFR 578. It is a locally-administered data system used to record and analyze client, service and housing data for individuals and families who are homeless or at risk of homelessness. HMIS is a valuable resource because of its capacity to integrate and un-duplicate data across projects in a community. Aggregate HMIS data can be used to understand the size, characteristics, and needs of the homeless population at multiple levels: project, system, local, state, and national. The Annual Homeless Assessment Report (AHAR) is HUD's annual report that provides Congress with detailed data on individuals and households experiencing homelessness across the country each year. This report could not be written if communities were not able to provide HUD with reliable, aggregate data on the clients they serve.

In 2010 the U.S. Interagency Council on Homelessness (USICH) affirmed HMIS as the official method of measuring outcomes in its Opening Doors: Federal Strategic Plan to Prevent and End Homelessness. Since then many of the federal agencies that provide McKinney-Vento Act and other sources of funding for services to specific homeless populations have joined together and are working with HUD to coordinate the effort.

HMIS is now used by the federal partners and their respective programs in the effort to end Homelessness, which include:

- U.S. Department of Health and Human Services (HHS)
- U.S. Department of Housing and Urban Development (HUD)
- U.S. Department of Veterans Affairs

The HMIS Data Standards provide communities with baseline data collection requirements developed by each of these federal partners. The HMIS Data Standards Manual is designed for CoC's, HMIS Lead Agencies, HMIS System Administrators, and HMIS Users to help them understand the data elements that are required in an HMIS to meet participation and reporting requirements established by HUD and the federal partners.

HUD is responsible for coordinating the collection of data, oversee HMIS rules and regulations, and report to Congress through the AHAR, and will continue to manage the HMIS regulations provide support and guidance to local CoC's and HMIS Lead Agency Agencies, and provide guidance to users in collaboration with the federal partner agencies. The 2014 release of the Data Dictionary and Manual is the first joint publication of HUD and the federal partners and is intended to provide guidance to communities around federal expectations for HMIS. The HMIS Data Standards Manual was updated most recently in July 2017.

1.2 San Diego's Continuum of Care

The San Diego CoC includes all of the geography within San Diego County, including 18 incorporated cities and all unincorporated areas. For HMIS purposes, the San Diego Region is often described as the City of San Diego and the outlying County, or as composed of five sub regions, Central, East, South, North Inland, and North Coastal areas. These boundaries contain other HUD designated program

components, including multiple Housing Authorities, thirteen (13) HUD geocode areas, three (3) local Emergency Solutions Grant (ESG) areas, ten (10) communities eligible for State ESG funds, as well as federally designated Community Development Block Grant (CDBG) entitlement areas, Housing Opportunities for Persons With AIDS (HOPWA) programs, HOME Investment Partnerships Programs (HOME), Veterans Administration (VA) service areas, Projects for Assistance in Transition from Homelessness (PATH), and Runaway and Homeless Youth (RHY) programs. The CoC's primary area of operations within the CoC geography includes the areas served by the program components listed above. This geography is referred to as the San Diego CoC Region (Region).

1.3 San Diego's HMIS Software

The HMIS provides homeless service providers throughout the Region with a collaborative approach to data collection and client management.

The CoC selected "ServicePoint," a web-based HMIS software owned by Mediware Information Systems, to be the HMIS software of record. It empowers human services providers, agencies, coalitions, and communities to manage real-time client and services data. The RTFH contracts directly with Mediware Information Systems for this software and supports end-users with help desk, ongoing training, and project customization including development of project-specific assessments and settings. The RTFH works directly with Participating Agencies to identify needs and requirements for custom reports developed by the RTFH or canned reports made available by Mediware Information Systems.

ServicePoint features:

- Combine the ease of the internet and the performance of a powerful database;
- Protects client confidentiality by carefully restricting access;
- Has a robust client and referral tracking, case management, agency and project indexing;
- Has an advanced reporting tool to understand and use key data;
- Facilitates the secure sharing of data to help providers to effectively and efficiently perform client case management;
- Ensures client, project, and agency-level data is available and accessible to all Participating Agencies in accordance with Federal, State, and local data sharing policies;
- User-friendly, requiring a minimum learning curve for data entry and generation of reports;
- Ensures project and agency-wide reports are easily produced by agencies; and
- Ensures providers can record detailed client profiles, assessments, referrals, history, and outcomes.

Benefits to Participating Agencies:

- Increased ability to prepare statistical and programmatic reports for funders, boards, and other stakeholders;
- Saves staff time needed to gather client data;
- Formulates statistics and completes funding reports;
- Increases ability to track client outcomes and measures the success of services provided;
- Increases ability to work collaboratively and to cooperate with other agencies to achieve meaningful results; and
- Significantly improves efficiency in delivering and managing services, resulting in tangible cost savings.

Benefits to Clients:

- Provides a comprehensive view of the client, minimizing data collection;

- Provides an ability to comprehensively coordinate client care in real time; and
- Provides a single client record for improved provision of services.

2. HMIS LEAD AGENCY MISSION AND CONTACT INFORMATION

2.1 Regional Task Force on the Homeless (RTFH)

RTFH Mission

"To provide comprehensive data and trusted analysis that empowers the entire community to identify, implement, and support efforts to prevent and alleviate homelessness."

The Regional Task Force on the Homeless (RTFH) serves as the HMIS Lead Agency. In that capacity, RTFH is responsible for the management and development of the HMIS implementation. Under the guidance of the RTFH, agencies with homeless-dedicated programs are required to participate in the HMIS to support local data collection, service, and planning functions within the CoC's jurisdiction. Participating Agencies are defined as those agencies that have signed Agency Participation Agreements. The RTFH encourages Agencies that provide beds and services funded by other federal, state, local, or private resources to also participate in the HMIS.

Contact Information

Regional Task Force on the Homeless
4699 Murphy Canyon Road
San Diego, California 92123
Telephone: (858) 292-7627
Fax: (858) 292-7627
Email: Support@RTFHSD.org
Website: www.RTFHSD.org

Role	Function
Executive Director	• CoC HMIS Lead Agency • HMIS direction & oversight
HMIS System Administrator	• General HMIS administration • Oversight and supervision of HMIS Technical Team
HMIS Security Officer	• Monitor security of the HMIS • Ensure HMIS Lead Agency and Participating Agency compliance with Security Policies and Procedures
HMIS Technical Team	
HMIS Project Analyst	• General technical support for HMIS issues related to end-user access, troubleshooting, information requests, system functionality errors, etc. • End-user training
HMIS Data Analyst	• Issues related to data quality, data analysis, mandated reports, report failure, etc.

3. ROLES AND RESPONSIBILITIES

3.1 General Compliance, Documentation, and Officials

General Compliance, Documentation, and Officials Policy

The HMIS Lead Agency will adopt and implement the Physical, Technical, and Administrative safeguards for the protection of information contained in the HMIS. The HMIS Lead Agency will be responsible for the organization and management of the HMIS as outlined in the CoC's Memorandum of Understanding with the HMIS Lead Agency.

Participating Agencies shall adopt, at a minimum, the HMIS Policies and Procedures as a baseline or develop their own where not in conflict with this Policy.

HMIS Lead Agency Procedure

The HMIS Lead Agency is responsible for all system-wide policies, procedures, communication, and coordination. It is also the primary contact with the software vendor, and is expected to implement all necessary system-wide changes and updates. The system is defined as the HMIS system.

In addition, the HMIS Lead Agency is responsible for all privacy concerns relating to the HMIS and serves as the Privacy Official (PO) for the CoC.

The HMIS Lead Agency may amend the HMIS Policies and Procedures at any time, subject to the approval of the Data Advisory Committee (DAC). The DAC may bring issues to the Governance Board as necessary for resolution.

Amendments may affect data that had been entered in the HMIS before the effective date of any such amendment. This policy is consistent with current standards for HMIS as outlined in the most recently published HMIS Data Standards Manual.

The HMIS Lead Agency Executive Director (or his/her designee) will serve as the HMIS System Administrator whose primary function is to manage the HMIS in accordance with HUD and other federal agency guidelines.

HMIS Lead Agency System Administrator

The HMIS System Administrator shall:

- Provide training support to Participating Agencies by determining training needs of HMIS end-users, developing training materials, and providing technical support by troubleshooting data with Participating Agencies;
- Manage end-user accounts and access controls;
- Identify and develop system enhancements and communicate enhancements and/or changes to Participating Agencies;
- Communicate system-related information to Participating Agencies;
- Develop and modify reports for end-users as requested;
- Maintain files of the name and contact information of the current Security Officer for each Participating Agency;
- Ensure, through contract or instruction, that Participating Agencies will:

- Identify a Participating Agency Administrator who serves as the primary contact between the Participating Agency and the HMIS Lead Agency on matters outlined in this document including but not limited to:

    - Providing HMIS support for their agency and escalating unresolved issues to the HMIS System Administrator;

    - Notify all end-users from their agency of system-wide changes and other relevant information;

    - Ensure all end-users from their agency are trained in the HMIS;

    - Notifies the HMIS Lead Agency of personnel changes;

    - Monitors their agency's compliance with standards of confidentiality and data collection, entry and retrieval;

    - Ensures all authorized end-users from their agency complete training before requesting access to the HMIS and understand and adhere to the HMIS User Agreement;

    - Ensures Participating Agency adherence to HMIS Policies and Procedures; and

    - Makes continuous efforts to detect violations of privacy and security and respond to any indication or report of violations.

HMIS Lead Agency Security Officer

The HMIS Lead Agency will name one employee as HMIS Security Officer.

The duties of the HMIS Lead Agency Security Officer will be included in the individual's job description and must be signed by the HMIS Security Officer to indicate understanding and acceptance of these responsibilities. The HMIS Security Officer's contact information is incorporated into these HMIS Policies and Procedures by reference.

Duties include, but are not limited to:

- Work cooperatively with the HMIS System Administrator to review the HMIS Policies and Procedures on an annual basis or at the time of any changes to the following:

    - The security management process, the methods of data exchange, and any HMIS data or technical requirements issued by HUD and the federal partners;

    - In the event that changes are required to the HMIS Privacy and Security Policies and Procedures, the Security Officer will work with the HMIS System Administrator to develop recommendations for review, modification, and approval by the DAC;

    - Review the HMIS Security Certification Checklist annually, test the HMIS Lead Agency security practices for compliance, and work with the HMIS System Administrator to coordinate communication streams;

    - Certify that the HMIS Lead Agency adheres to the HMIS Privacy and Security Policies and Procedures;

    - Demonstrate risk in reduction over time;

- Develop mitigation plans for any identified security shortfall, including milestones to demonstrate the reductions in risk over time;

- Implement any approved plan for mitigation of shortfalls and provide appropriate updates on progress to the DAC;

- Respond to any security questions, requests, or security breaches, and communicate security-related HMIS information to each Participating Agency Security Officer and the Participating Agency's end-users, and will inform the DAC as appropriate; and

- Monitor HMIS Audit Reports monthly.

- The HMIS Security Officer and any user employed or retained by the HMIS Lead Agency able to access HMIS data will undergo criminal background verification. Records of the completed background checks (though not the results) are subject to inspection;

  - The HMIS Lead Agency will follow its own policies regarding hiring individuals with criminal justice histories, as long as they comply with all relevant laws; and

  - The HMIS Lead Agency will not hire individuals whose background checks reveal criminal histories related to identity theft or fraud. The HMIS Lead Agency will manage the results of any background checks conducted on a case-by-case basis.

- The HMIS Lead Agency will maintain all policies and procedures, including changes, in either electronic or paper format, for a period of six (6) years after creation or most recent revision and adoption; and

- The HMIS Lead Agency will also document all changes to electronic systems such as server change out, new applications, changes in technology vendors or any substantive change to the infrastructure of systems.

Participating Agency Procedure

Participating Agency shall adopt, at a minimum, the HMIS Privacy and Security Policies as a baseline or develop their own where not in conflict with the HMIS Privacy and Security Policies and Procedures.

- Participating Agencies may require more rigorous privacy standards but they must, at minimum, meet and not contradict the HMIS Privacy and Security Policies and Procedures;

- Participating Agencies that elect to adopt different Privacy and Security Policies shall attach a copy of the policies to the HMIS Security Certification Checklist;

- More stringent mandates shall be submitted to the HMIS System Administrator for incorporation into these policies where applicable;

- Participating Agencies shall annually self-certify compliance with the HMIS Privacy and Security Policies and Procedures unless they have developed and operate under their own;

- Participating Agencies shall record compliance with the HMIS Privacy and Security Policies and Procedures, or their own if so elected, through completion of the HMIS Security Certification Checklist;

- Failure to submit the HMIS Security Certification Checklist within 30 (thirty) days of its due date in any given year will be considered to be a violation of the terms of the HMIS Agency Participation Agreement and these policies;

- Each Participating Agency shall indicate within the HMIS Security Certification Checklist, whether or not it has:
    - Adopted the HMIS Privacy and Security Policies and Procedures; or
    - Adopted different Privacy and Security Policies and Procedures that meet the requirements outlined in the HMIS Privacy and Security Policies and Procedures.
    - Participating Agencies must maintain documentation regarding changes to their Security and Privacy policies for a period of six (6) years beyond adoption.

A Participating Agency's Privacy and Security Policies shall at minimum:

- Specify the purpose for collecting the information;
- Specify all potential uses and disclosures of information;
- Specify the time period for which the hard copy and electronic data will be retained at the organization;
- Specify the method for disposing of data or removing identifiers from personal information that is not in current use;
- State the process and applicability of amendments;
- Offer reasonable accommodations for persons with disabilities and/or language barriers;
- Allow the client the right to inspect and to have a copy of their client record and offer to explain any information the individual may not understand;
- Include reasons and conditions when a Participating Agency would not release information to any party not authorized by the client; and
- Specify a procedure for accepting and considering questions or complaints about the Privacy and Security Policy.

Participating Agency Data Owner

The Participating Agency Data Owner is an employee of the Participating Agency who is ultimately responsible for the protection and use of the data entered into the HMIS and shall:

- Develop Participating Agency procedures for determining and granting access to systems that comply with applicable Federal and State laws that govern the privacy and confidentiality of data;
    - Participating Agency may impose greater restrictions not specifically covered by Federal or State law, or other regulations; and
    - Data sharing restrictions requested by the client and accepted by the Participating Agency may also impose a data access restriction.
- Monitor end-user data access; and
- Determine Participating Agency data retention schedule.

Each Participating Agency is responsible for conducting a security review annually and certifying that each participating project is in compliance with minimum standards of the HMIS Privacy and

Security Policies and Procedures and HMIS Data and Technical Standards. Participating Agencies shall include a provision in their policies and procedures to comply with this policy.

Participating Agency network design should allow for uninterrupted communication between workstations and the internet. All communication between servers should be designed to be performed on a Local Area Network (LAN).

Participating Agency hard copies of data stored in HMIS shall be treated in the following manner:

- End-users are responsible for maintaining the security of all client data extracted from the HMIS, including hard copies, and any data collected for purpose of data entry into the HMIS;
- Hard copy records containing Personally Identifiable Information (PII) must be disposed of through means such as cross cut shredding and pulverizing or use of a Certified Destruction Vendor;
- Records shall be kept in individual locked files or in rooms that are locked when not in use;
- Records in use (i.e. on the desktop) shall be maintained in such a manner as to prevent exposure of information to anyone other than the user directly utilizing the record;
- End-users or other staff shall not remove records or other information from their place of business without written permission from appropriate supervisory staff;
    - Written permission must specify the reason for removal of information and handling procedures while off site;
    - Staff shall maintain information in a secure manner while off site; and
    - Records transferred from one location to another physical location (i.e., different building), must be placed in sealed envelopes and utilize a tracking receipt to capture in transit responsibility up to and including delivery of records.
- Faxes or other printed documents with HMIS information shall not be left unattended; and
    - Fax machines and printers shall be kept in secure areas.
- After completion of faxing, copying or printing information, documents should be removed from the machines immediately; and
    - The Participating Agency Data Owner may delegate the responsibility of the day-to-day maintenance of the data, which then becomes the responsibility of the Participating Agency Administrator (defined below).

Participating Agency Administrator

Each Participating Agency must designate an Agency Administrator and a backup Agency Administrator responsible for the oversight of all activities that generate or have access to client data in the HMIS to ensure adherence to HMIS Policies and Procedures in this document. Changes to Agency Administrators must be reported to the HMIS Lead Agency within ten (10) business days.

The Participating Agency Administrator shall be responsible for:

- Reviewing the Participating Agency's Privacy and Security Policies to ensure consistency

with the HMIS Privacy and Security Policies and Procedures;

- Providing oversight of all personnel who generate or have access to client data in the HMIS for HMIS Policy & Procedure compliance;
- Serving as the primary contact between end-users and the HMIS System Administrator;
- Providing Participating Agency technical support by troubleshooting data and escalating unresolved issues to the HMIS System Administrator;
- Notifying members of their Participating Agency of any system-wide changes and other relevant information;
- Offering training support to Participating Agency end-users when approved by the HMIS Lead Agency (ex. “Train-the-Trainer”);
- Notifying the HMIS Lead Agency of Participating Agency personnel changes;
- Monitoring compliance with standards of confidentiality and data collection, entry, and retrieval related to the HMIS;
- Ensuring all authorized end-users are trained before being granted access to the system and are adhering to the HMIS User Agreement (Appendix B);
- Ensuring Participating Agency adherence to internal Privacy and Security Policies and Procedures and contractual privacy and security procedures;
- Making continuous efforts to detect violations of privacy and security of the HMIS and respond to any indication or report of violations; and
- Providing the name and contact information of the Participating Agency’s Security Officer.

Participating Agency Security Officer

Each Participating Agency must designate an Agency Security Officer who will serve as the Participating Agency Security Officer for the HMIS and is responsible for ensuring compliance with the security standards outlined in this document.

Participating Agencies must provide the name and contact information of the Agency Security Officer to the HMIS Lead Agency and report changes to that information within ten (10) business days.

Participating Agency Security Officer responsibilities include but are not limited to:

- Review and testing the Participating Agency’s security practices for compliance;
- Certify the Participating Agency’s adherence to the HMIS Security Policy and Procedures;
- Develop mitigation plans for identified security shortfalls including milestones;
- Demonstrate reduction in risk over time;
- Complete HMIS Security Certification Checklist and submit it within thirty (30) days of its due date to the HMIS Security Officer;

- Communicate any security questions, requests, or security breaches to the Participating Agency Administrator;

- Communicate security-related HMIS information relayed from the HMIS Security Officer to the Participating Agency end-users; and

- Complete security training offered by the HMIS Lead Agency.

3.2 Monitoring and Auditing

Monitoring and Auditing Policy

The HMIS Lead Agency will develop monitoring procedures so regular checks are performed on system usage, security attack vectors, and other risks to information. Mitigation plans, based on risks, shall be developed to reduce risk associated with an event or identified system vulnerability.

The HMIS Lead Agency will develop an investigation process including a communication plan for informing and coordinating with the DAC and Agency Administrators and/or Security Contacts.

Procedure

The HMIS Lead Agency will develop a monitoring and investigation process including a communication plan for informing the DAC, Participating Agency Administrators, and Participating Agency Security Officers of issues related to privacy and security including:

- Identification of risks associated with the connection between the HMIS and Participating Agencies shall be addressed in contractual language to ensure the reduction of risk;

- Development and implementation of Participating Agency requirements for reporting and investigation of complaints on privacy or security policies, security incidents, or privacy breaches;

    - The HMIS Lead Agency will communicate any reported security breaches or failures to the Participating Agency Security Officer with mutual clients within 24 hours of the discovery.

- Privacy and Security Policy and Procedure concerns reported to the HMIS Lead Agency; and

- Processes established by Participating Agencies for receiving and reviewing complaints from clients about potential violations of HMIS policies.

The HMIS software vendor will monitor HMIS for security breaches and suspected system security failures.

- Breaches or system security failures will be reported to the HMIS Security Officer and HMIS System Administrator;

- Corrective actions, potentially in the form of sanctions, may be implemented if necessary to mitigate the identified risk; and

- Any sanction by RTFH may be appealed, after the completion of investigation, to the DAC for relief of the severity of the penalty.

Participating Agency Procedure

All suspected breach of security, or any incident in which unauthorized use or disclosure of information has occurred, or where the HMIS may have been accessed or used in a manner inconsistent with the HMIS Policies and Procedures, must be reported to the HMIS Security Officer.

Procedures include:

- HMIS end-users are obligated to report to their Participating Agency's HMIS Security Officer suspected instances of noncompliance with established HMIS Policies and Procedures that may leave HMIS data vulnerable to intrusion;
- The HMIS Lead Agency is responsible for reporting security incidents involving the real or potential intrusion of HMIS to the DAC;
- Each Participating Agency is responsible for reporting any security incidents involving the real or potential intrusion to the HMIS Security Officer;
- Participating Agencies will regularly check their system for security breaches and failures by running reports such as User Login, User Information, and Audit Report. Any such breaches or failures will be reported to the HMIS System Administrator and HMIS Security Officer;
- The HMIS Lead Agency will notify the DAC of critical security breaches that require necessary corrective action to mitigate the identified risk;
- End-users must report security violations, including suspected uncorroborated violations, as soon as discovered to their Participating Agency Administrator or Participating Agency Security Officer;
- Participating Agency will relay reports within one (1) business day of receipt to the HMIS Lead Agency Security Officer
- A complete investigation, or determine and mitigation actions, is not required prior to the initial reporting;
- Participating Agencies shall report any violation of the HMIS Policies and Procedures to the HMIS Lead Agency; and
- Reporting does not preclude or substitute for any corrective actions determined by Participating Agency.

Each Participating Agency is responsible for monitoring its projects to ensure the standards set forth in these HMIS Policies and Procedures are met to the greatest possible extent, and that data quality issues are quickly identified and resolved. Each Participating Agency is responsible for addressing and correcting any issues identified through the monitoring process.

Any Participating Agency failing to meet data quality standards will be in violation of the terms of the HMIS Agency Participation Agreement.

Participating Agency Security Officer will be responsible for:

- Testing its security practices; and
- Completing an HMIS Security Certification Checklist;

- Failure to submit the Checklist within thirty (30) days of its due date in any given year may require the Participating Agency to undergo graduated sanctions as defined by the CoC;
- Participating Agencies may appeal sanctions to the DAC;
- The DAC may sanction the Participating Agency, including revocation of access to the HMIS and CoC funding for that year, until such time as the DAC determines the Participating Agency has achieved compliance. The DAC may elevate issues to the Governance Board.

The Participating Agency's HMIS Security Certification Checklist will indicate whether it meets each of the requirements outlined in the HMIS Privacy and Security Policies and Procedures.

If a requirement is not met at the time of execution of the HMIS Agency Participation Agreement, or at the time of annual certifications thereafter, the Participating Agency must establish a date no later than three (3) months from the certification review date by which that requirement will be met. An updated HMIS Security Certification Checklist indicating full compliance will be provided to the HMIS Lead Agency by the target date or the Participating Agency will be in violation of the terms of the HMIS Participation Agreement and could be subject to sanctions.

4. IMPLEMENTATION

4.1 HMIS Agency Participation Agreement

HMIS Agency Participation Agreement Policy

The Executive Director (and/or designee) of any Participating Agency shall execute, comply, and enforce the HMIS Agency Participation Agreement (Appendix A).

Procedure

Participating Agencies wishing to participate in the HMIS must sign an HMIS Agency Participation Agreement (Appendix A) before any end-user is allowed access to the HMIS.

4.2 HMIS User Agreement

HMIS User Agreement Policy

End-users of Participating Agencies shall execute, and comply with the HMIS User Agreement (Appendix B).

Procedure

The HMIS System Administrator shall provide end-users authorized by Participating Agencies with an HMIS User Agreement (Appendix B) for signature. The HMIS System Administrator will maintain HMIS User Agreements of all end-users.

The Participating Agency end-user must sign an HMIS User Agreement and be trained by the HMIS Lead Agency before being granted access to the HMIS. The HMIS Lead Agency will train the Participating Agency end-users to use the HMIS software upon execution of the HMIS Participation Agreement. HMIS access will only be granted after required training is satisfactorily completed. Participating Agency end-user access and passwords will be granted upon completion of mandatory training.

4.3 HMIS Data Collection and Data Quality

HMIS Data Collection and Data Quality Policy

Participating Agencies shall enter data into the HMIS in real time or within three (3) business days of collecting the information. At minimum, data entered must include Universal Data Elements (UDEs). Program Specific Data Elements (PSDEs) are required to be entered as outlined in the most recently published HMIS Data Standards Manual. Participating Agencies may also be required to collect additional data fields locally identified to support specific regional projects.

Procedure

Data Entry

Participating Agencies must enter:

- Universal Data Elements (UDEs) as documented in the most recently published HMIS Data Standards Manual as the minimum set of data elements for all clients served by projects;
- Program-Specific Data Elements (PSDEs) as required by the Participating Agency and/or funder as documented in the most recently published HMIS Data Standards Manual;
- Participating Agencies must also collect data fields locally identified for specific projects; and

- "Client Doesn't Know" and "Client Refused" must only be used to indicate the client did not know or the client refused to provide the data. "Data Not Collected" must only be used to indicate the data was not collected.

Data Quality and Completeness

All data entered into the HMIS shall be complete. Partially complete or missing data (e.g., digit(s) in a SSN, year of birth, information on disability or veteran status) can negatively affect the ability to provide comprehensive care to clients. Missing data could mean the client does not receive services that could help them become permanently housed and end their homelessness.

The goal is to collect one hundred percent (100%) of all data elements. However, the CoC recognizes this may not be possible in all cases. Therefore, it has established an acceptable range of Missing (null) and Incomplete (Client Doesn't Know/Client Refused) responses, depending on the data element and the type of project entering data.

All projects using the HMIS shall enter data on one hundred percent (100%) of the clients they serve.

Acceptable Range of Missing and Incomplete Responses:

Data Element	Required For	Residential Projects		Street Outreach & Supportive Services Only Projects	
		Missing	Incomplete	Missing	Incomplete
Universal Data Elements (UDEs):					
Name	All	<5%	<7%	<10%	<12%
Social Security Number	All	<5%	<7%	<10%	<12%
Date of Birth	All	<5%	<7%	<10%	<12%
Race	All	<5%	7%	<10%	<12%
Ethnicity	All	<5%	<7%	<10%	<12%
Gender	All	<5%	<7%	<10%	<12%
Veteran Status	Adults	<5%	<7%	<10%	<12%
Disabling Condition (Y/N)	Adults	<5%	<7%	<10%	<12%
Residence Prior to Project Entry	Adults/HoH	<5%	<7%	<10%	<12%
Length of Stay in Previous Place	Adults/HoH	<5%	<7%	<10%	<12%
Destination (Exit)	Adults/HoH at Exit	<5%	<7%	<10%	<12%
Relationship to Head of Household	All	<5%	<7%	<10%	<12%
Client Location	HoH ONLY	<5%	<7%	<10%	<12%
Continuously Homeless for at Least One Year	Adults/HoH	<5%	<7%	<10%	<12%
Number of Times Client Homeless in Past 3 Years	Adults/HoH	<5%	<7%	<10%	<12%
If 4 or More (for Above), Total Number of Months	Adults/HoH 4+ONLY	<5%	<7%	<10%	<12%
Total Number Months Cont. Homeless Prior to Entry	Adults/HoH	<5%	<7%	<10%	<12%
Status Documented?	Adults/HoH	<5%	<7%	<10%	<12%
Additional Data Elements:					
Domestic Violence Victim/Survivor	Adults/HoH	<5%	<7%	<10%	<12%
Service	Adults/HoH	<5%	<7%	<10%	<12%
Income Received (Y/N)	Adults/HoH	<5%	<7%	<10%	<12%

Non-Cash Benefit Received (Y/N)	Adults/HoH	<5%	<7%	<10%	<12%
Covered by Health Insurance (Y/N)	Adults/HoH	<5%	<7%	<10%	<12%
HUD Verification: (Elements measure completeness at Entry ONLY)					
Disability Type	All	<5%	<7%	<10%	<12%
Income Source	All	<5%	<7%	<10%	<12%
Income Amount (for all valid sources)	Adults/HoH	<5%	<7%	<10%	<12%
Non-Cash Source	Adults/HoH Rec Inc. = Y	<5%	<7%	<10%	<12%
Health Insurance Type	Adults/HoH	<5%	<7%	<10%	<12%
Other Federally Mandated Data Elements: (Based on Funding Source, as applicable)					
Various Data Elements (as outlined in the most recently published HMIS Data Standards)	As Applicable	<5%	<7%	<10%	<12%

Bed/Unit Utilization Rates

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

- Emergency Shelters (ES): 75%-105%;
- Transitional Housing (TH): 80%-105%; and
- Permanent Supportive Housing (PSH): 85%-105%.

Projects outside of this acceptable range may provide a brief explanation to the HMIS Lead Agency.

New projects may require time to reach the projected occupancy numbers and will not be expected them to meet the utilization rate requirement during the project's first operating year.

Timeliness

Participating Agencies are expected to enter data into the HMIS in real-time or within three (3) business days of collection.

- Changes for clients active in the HMIS should occur at point of service or within thirty (30) business days a Participating Agency learns of a material change.

Accuracy

All data entered into the HMIS shall be a reflection of information provided by the client. Intentionally recording inaccurate information is strictly prohibited, unless in cases when a client refuses to provide correct personal information (see below). All data in HMIS shall be collected and entered in a common and consistent manner across all projects.

Only when a client refuses to provide personal information and the program funder does not prohibit it, is it permissible to enter client data under an alias.

- The Participating Agency is responsible to the funding source for any duplication of services that results from knowingly entering false information (i.e., hiding the actual name under an alias).

Monitoring

The HMIS Lead Agency shall conduct annual reviews and upon request of the DAC and/or Governance Board provide project-level monitoring reports to the DAC, Evaluation Committee, or

the general public for transparency and for the purpose of ensuring projects comply with standards outlined by local, state, and federal partners.

Unless a more accurate method is available (e.g., client interview, third party verification, etc.), a sampling of client source documentation can be used to measure the data accuracy rate. The HMIS Lead Agency may request client files or intake forms during the annual HMIS Security Certification Checklist process and compare the source information to the information in the HMIS. Only those parts of the client file containing the required information will be reviewed, excluding any non-relevant, personal, or Participating Agency-specific information.

The HMIS Lead Agency shall provide Participating Agencies the training and tools necessary for Participating Agencies to self-monitor project performance.

4.4 Technical and Security Standards

Technical and Security Standards Policy

Participating Agencies must meet the technical standards outlined below to participate in the HMIS.

Procedure

Supported Browser Brands

Microsoft Internet Explorer versions 8, 9, 10
Google Chrome (recommended)
Mozilla Firefox
Apple Safari

Java

Required	Recommended
Any version of Java	Version 7 release 76 (32 bit)

Mobile Devices

Apple iPad with latest version of IOS; version 8.1.2

Operating Systems

Operating System	Required	Recommended
Windows Vista	Any version of Internet Explorer 2 GB of RAM	Any version of Internet Explorer other than version 9. 4 GB of RAM
Windows 7	Version 32bit 2GB of RAM	Windows 7 version 64bit 4 GB of RAM
Windows 8	Run with most version of Java (version Java 7 release 76), with "Modern" version of Internet Explorer	Run with most version of Java (version Java 7 release 76), with "Desktop" version of Internet Explorer
Windows XP, Windows 8 RT, and Windows 10	Not recommended operating systems due to a lack of compatibility and support with ServicePoint.	

Connection to the Internet is the sole responsibility of the Participating Agency and is a requirement to participate in the HMIS.

Participating Agency network design should allow for uninterrupted communication between workstations and the internet. All communication between servers should be designed to be performed on Local Area Network (LAN).

For security purposes, all computers must have the following:

- An updated and adequate firewall protection; and
- Virus protection software in which virus definition must be updated regularly.

Similarly, Participating Agencies are required to establish a policy for disposal of or anonymization of information not in current use seven (7) years after the information was created or last changed unless prohibited.

4.5 Maintenance of Onsite Computer Equipment

Maintenance of Onsite Computer Equipment Policy

Participating Agencies will commit to a reasonable schedule of equipment maintenance to sustain an efficient level of system operation.

Procedure

The Executive Director (and/or designee) of Participating Agencies will be responsible for the maintenance and disposal of onsite computer equipment. This includes:

- Purchase of and upgrades to all existing and new computer equipment for utilization in the system;
- Workstations accessing the system must have a username/password to log onto Microsoft Windows and/or Mac Operating System(s);
- Workstation accessing system must have locking, password-protected screen saver; and
- All workstations and computer hardware (including Participating Agency network equipment) must be stored in a secure location (locked office area).

4.6 HMIS Technical Support Protocol

HMIS Technical Support Protocol Policy

The HMIS Lead Agency will provide technical support to all Participating Agencies as needed.

Procedure

- Participating Agency end-users should first seek technical support from the Participating Agency Administrator;
- If more expertise is required to troubleshoot the issue, the Participating Agency Administrator or end-user will contact the HMIS Lead Agency's Technical Team;
- Technical support hours are Monday through Friday (excluding holidays) from 8:00 am to 5:00 pm;
- The Participating Agency Administrator will work closely with the HMIS Lead Agency to identify details of technical problems experienced;
- The HMIS System Administrator or Technical Team will respond to all email inquiries and issues within one (1) business day but no more than three (3) business days.

4.7 System Availability

System Availability Policy

The HMIS will make all attempts to be available to Participating Agency end-users Monday – Friday during normal business hours, holidays excluded. The HMIS Vendor or the HMIS Lead Agency will inform Participating Agency end-users of any interruption in service as soon as reasonable.

Procedure

- The HMIS Vendor will communicate to the HMIS Lead Agency any necessary downtime for system upgrades and patches;
- In the event it is determined the HMIS accessibility is disabled system-wide, the HMIS Lead Agency will work closely with the HMIS Vendor to resolve any issues; and
- The HMIS Lead Agency will send communication to the Participating Agency Administrators within two (2) hours of problem awareness and provide an estimated time of system availability.

4.8 HMIS Participation Fees

HMIS Participation Fees Policy

HMIS participation fees include the cost of Participating Agency end-user licenses as required by the HMIS Vendor. In addition to costs associated with licensing, the HMIS Lead Agency may charge reasonable technical support fees. Depending on funding availability, the HMIS Lead Agency may, at its discretion, waive or reduce fees to encourage HMIS participation for Participating Agencies.

Procedure

The HMIS Fee Schedule will be included as an attachment to the HMIS Participation Agreement (Appendix A). The HMIS fee structure will be reviewed by the DAC annually. Changes to the HMIS Fee Structure must be approved by the Governance Board.

4.9 Training, Ethics, and Sanctions

Training, Ethics, and Sanctions Policy

All Participating Agency end-users shall receive privacy, security, ethics, and sanctions policies training related to the HMIS prior to accessing the system.

Each Participating Agency end-user must complete the required trainings relevant to their user role prior to receiving access to the HMIS.

Procedure

Training

The HMIS Lead Agency will provide Participating Agency end-users a copy of the HMIS Policies and Procedures. Additionally, the HMIS Lead Agency will provide:

- Basic User Training to new Participating Agency end-users;
- Basic User Training to Participating Agency Administrators for support of agency personnel, if applicable; and

- Training in security-related requirements such as:
    - Prohibition on sharing usernames or passwords;
    - Allowing others to occupy their work station (use their computer) when logged into the HMIS; and
    - Writing/Posting user IDs and/or password where other may access them.

Participating Agency End-users must successfully complete the new user training and pass the exam to demonstrate proficiency in the system and understanding of the HMIS Policies and Procedures.

Trainings

Module/Course	Module/Course Detail	Required
New User Training		
HMIS 101	Review of HMIS background and HMIS Data and Technical Standards	All new Participating Agency end-users, one time.
HMIS Privacy, Security, and Ethics	Review of HMIS Policies and Procedures including Privacy and Security standards, authorization forms, ethics, and confidentiality	All new Participating Agency end-users one-time, and existing end-users annually.
HMIS Basic User	Introduction to using the HMIS, including how to navigate and use the basic workflow	All new Participating Agency end-users, one time.
HMIS Workflows	Navigation, system use, and HMIS Data and Technical Standards information tailored for each unique HMIS workflow	All new Participating Agency end-users, one-time as necessary per workflow.
Other Trainings		
HMIS Refresher	Workflow-specific review of navigating and using the HMIS, review of HMIS Data and Technical Standards	All existing Participating Agency end-users, annually.
Participating Agency Administrator	Navigating client-level and administrative level data	All new Participating Agency Administrators and backup Participating Agency Administrators, one time.
Reports	Running and understanding management reports such as Advanced Reporting Tool (ART) and canned reports	All Participating Agency end-users who run reports, one time.

The HMIS System Administrator shall maintain documentation that each Participating Agency end-user has completed training prior to gaining system access and annually thereafter.

Sanctions

The HMIS Lead Agency will apply progressive discipline to HMIS Lead Agency workforce members who violate HMIS Policies and Procedures or law.

Participating Agency staff who violate HMIS Policies and Procedures are subject to revocation of HMIS access and may be subject to criminal investigation.

Regardless of the Participating Agency end-user's position, discipline shall be based on:

- The severity of the incident;
- The asset value;
- Impact on funding;
- Mitigating circumstances;

- Repetitive nature of the incident; and
- Previous behavior.

Progressive Discipline Severity Groups

Group 1	• Not signing off HMIS when leaving a work area; • Inadvertent disclosure of HMIS information to wrong individual; and • Failure to follow appropriate guidelines for use of fax, mailing, email, computer or other transmission of client information causing a disclosure to an unintended recipient.
Group 2	• Sharing password; and • Accessing confidential information such as medical, billing or demographic information on a client the Participating Agency end-user has no job-related responsibility for, including friends, family, and the Participating Agency end-user's own record.
Group 3	• Using a coworkers password without their knowledge; • Releasing information for personal gain; • Releasing information with intent to harm the reputation of the individual or agency; and • Unauthorized or impermissible disclosure or access of: o Mental Health or Alcohol Drug information; o HIV test results; and o Records of sexual assault or any condition with special protection from the state or federal government.

Ethics

These general principles form the ethical or professional standards of conduct necessary for access to the HMIS. Each Participating Agency end-user shall adhere to the delivery of services with the highest standards of professionalism, integrity, and competence. This set of principles applies to all HMIS Participating Agency end-users including employees, temporary workers, and volunteers.

- Perform all duties in compliance with the spirit and letter of federal, state, and local laws, and avoid any involvement in illegal, unethical, or improper conduct;
- Conduct duties in conformance with all Participating Agency policies and procedures;
- Create a work environment that promotes open and honest communication, and encourages raising ethical concerns without fear of retribution or retaliation; and
- Assume responsibility for knowing, understanding, and having a practical working knowledge of the laws and regulations applicable to the job.

Participating Agency Procedure

Participating Agencies shall follow their own policies regarding background checks and hiring individuals (including volunteers) with criminal histories, as long as they comply with all relevant laws.

Participating Agencies that request access for individuals who have not been subject to a background check or where the Participating Agency allows individuals with criminal histories related to identity theft or fraud assume all liabilities resulting from those actions.

The Participating Agency Security Officer will document each Participating Agency end-user has completed security training prior to requesting system credentials and annually thereafter.

Participating Agencies are required to have a Code of Conduct or Ethics Policy that aligns with the HMIS Lead Agency's Ethics Policy. Annual ethics training is required and written confirmation that each HMIS end-user has acknowledged and agrees to the policy.

Each Participating Agency is required to have a Progressive Discipline Policy.

5. PRIVACY AND SECURITY

5.1 Privacy and Security

Privacy and Security Policy

The HMIS Privacy and Security Policies and Procedures apply to any person accessing HMIS data, however, Participating Agencies subject to more restrictive regulations will be honored. In order to incorporate any Participating Agency's more restrictive regulations, additional implementation elements may be utilized to provide a cohesive framework for policies and procedures.

Procedure

All HMIS Lead Agency assets (e.g., workstations, laptops, and other systems or devices that process and/or store HMIS information) must be protected by commercial anti-virus and Internet Security Software solutions.

- HMIS Lead Agency devices used to access HMIS shall utilize a firewall between the workstation and any external system including the Internet;
- Security solutions must be updated when new versions or releases become available;
- Security software and operating system patches shall be applied within a reasonable time when they become available; and
- Any HMIS information stored on media shall be encrypted.

Participating Agency End-users are advised that these policies do not allow any use that is unlawful or other applicable rules and regulations, or is specifically prohibited by this policy or another applicable agency policy.

Under no circumstances will end-users store Personally Identifiable Information (PII) on any personally owned media; end-users may not place PII on a work-owned USB drive for personal use.

PII and removable data devices (e.g., USB drives, CDs, and external drives) must be protected by appropriate physical means from modification, theft, or unauthorized access. Such records and confidential information contained therein remain subject to the HMIS Policies and Procedures. When these media have reached the end of their useful life, the data will be disposed of in a manner consistent with the procedures outlined in this policy.

Risk Analysis Management - HMIS Lead Agency Risk Analysis

The HMIS Security Officer, in conjunction with executive management, and the HMIS Lead Agency Privacy Officer, will perform a modified Security Risk Analysis (RA) in accordance with the National Institute of Standards and Technology (NIST). The minimum content of the RA shall consist of:

- List of assets (i.e. hardware, software, data, physical sites);
- Threats to each of the listed assets (ex.: hacking, malware, misuse of data, burglary);
- Likelihood threats and impact of threat exploitation; and
- Heat map of likelihood versus impact.

Any decisions on selection of security measures to reduce risk must be documented and based on the RA.

Lack of funds to support security measures may be a mitigating factor for the current fiscal term, however lack of funds should be addressed in a Short Term Security Mitigation Plan that is three (3) to five (5) years in implementation length and addresses funding.

HMIS Vendor

The CoC is responsible for the process and selection of the region's HMIS Vendor.

The HMIS Lead Agency is responsible for ensuring HMIS is operated in accordance with HMIS standards via the HMIS Vendor Contract.

The HMIS Lead Agency will include provisions in the HMIS Vendor contract requiring the physical security of the facilities and media storing the data is protected.

- The HMIS Vendor is required to take steps, consistent with the most current HMIS technical and security standards, to prevent unauthorized access to the data and the software (See Section 5.2 "Access Controls");
- The HMIS Lead Agency, through the HMIS Vendor contract, will take measures to ensure the system is protected from intrusion and risks to data loss is minimized;
- The HMIS Vendor will maintain software consistent with the most up-to-date HMIS technical and security standards:
    - The HMIS Vendor must retain a log of system changes and/or software version changes;
    - Security gaps or issues, identified by the HMIS Vendor or HMIS Lead Agency, shall be resolved in an expedient manner; and
    - The HMIS Lead Agency is responsible for ensuring all vendor-released enhancements, upgrades and bug fixes are applied promptly.

Participating Agencies shall be notified of changes by HMIS Lead Agency where appropriate.

Data Backup

HMIS Vendor shall store and maintain backup versions of the data in a separate physical location consistent with the most up-to-date HMIS technical and security standards. Examples include:

- HMIS Vendor servers on which the HMIS data is stored shall utilize firewalls;
- HMIS Vendor will also perform daily, weekly and monthly data backups;
    - Backups will be held offsite at a secondary (hot) data center;
        - Intra-day and day-end backups will be held on a local server as well as offsite at the secondary data center;
        - The failover function will be tested at least once per year and after each major system upgrade to ensure accurate continuous backup.

The HMIS Vendor shall:

- Maintain an accessible audit trail of the system;
    - Audit trail must capture user activity;
        - Activity will be monitored by the HMIS Lead Agency and the HMIS Lead Agency Security Officer will monitor audit reports monthly for security breaches or behavior inconsistent with this HMIS Privacy Policy and Procedure.

Physical Safeguards

Participating Agencies are contractually required to maintain procedures ensuring the physical security of facilities and media in which HMIS data is stored.

Technical Safeguards

Participating Agencies shall maintain and follow procedures to ensure a unique Participating Agency end-user nomenclature (one system-user per system-username).

Participating Agencies shall provide a procedure for password reset and a schema that prevents reuse or transfer of previously issued system credentials.

Participating Agencies shall develop, maintain, and follow procedures for accessing HMIS, regardless of the network or device ownership, which support data confidentiality and HMIS security.

Procedures must state:

- Individual Participating Agency end-users do not have exclusive rights to HMIS data;
- Participating Agency end-user access will be monitored;
- Participating Agencies shall maintain a current list of Participating Agency end-users; and
- How HMIS security will be ensured and the confidentiality of the data during collection, use, and transmission.

Participating Agency Procedure

- Conducting annual HMIS Privacy and Security Policy and Procedure reviews;
- Certifying each participating project is in compliance with the minimum standard of the HMIS Privacy and Security Policy and HMIS guidelines;
    - The HMIS Lead Agency retains the right to conduct at least annual site visits to ensure compliance;
        - Annual site visits will be announced and the HMIS Lead Agency may conduct unannounced site monitoring visits at its discretion; the HMIS Lead Agency will provide Participating Agencies 24 hours' notice for unannounced visits.
- Developing and maintaining Privacy and Security Policies and Procedures consistent with the most recently published HMIS Data Standards, and at minimum:
    - Mandate Participating Agency devices, used to access or store HMIS data, maintain a firewall between the device and any external system, including the Internet;
    - Mandate anti-virus software for Participating Agency end-users; and
    - Install, maintain, and update anti-virus software and internet security solutions such as firewalls, malware detection, and system intrusion detection for Participating Agency devices used to access HMIS;
        - Security solutions, and operating systems must be updated when new versions, patches or releases become available.

- Specify the Participating Agency Security Officer who is responsible for managing the security of Participating Agency hardware and software;

- Specify the frequency with which the software will be updated; and frequency of portable and desktop device security scanning; and

- Notify the HMIS Lead Agency of security issues within three (3) business days.

5.2 Access Controls

Access Controls Policy

The HMIS Lead Agency will develop and implement an integrated set of access controls to establish, monitor, audit, and terminate account access in supporting the confidentiality, availability, and integrity principles of information security. The HMIS Vendor is required to maintain access control mechanisms designed to reduce the risk of access to the system by unauthorized users. Access to the HMIS is governed by multiple layers of securities – passwords, user group assignment, and permissions as well as Public Key Infrastructure (PKI). Additionally, the HMIS will be structured in such a way as to prevent users from logging on to the system from more than one workstation at a time.

All connections to the HMIS shall be made over Secure Socket Layer (SSL) connections. Other connections to HMIS shall be limited to secure, direct, encrypted connections.

Procedure

Each Participating Agency end-user shall be granted a user access level in accordance with the type of information required for the Participating Agency user role.

- Participating Agencies are required to communicate to the HMIS System Administrator when a Participating Agency end-user's data needs change;

- HMIS System Administrator shall terminate access upon notification of termination of employee via direct contact from the Participating Agency;

- Anyone suspected of violating, or found to be in violation of HMIS Policies and Procedures shall have their access revoked;

    - Reestablishment of access may be granted after investigation or at the discretion of HMIS Lead Agency.

Role Based Access

The table below lists the levels of access tied to existing user roles across the HMIS. Customization of roles may be offered in consultation with, and approval of, the HMIS System Administrator.

HMIS Roles

HMIS User Role	Level of Access	Description
System Administrator	Access to all levels of data within the HMIS	This role will grant access to all system-wide data in order to support all Participating Agencies, meet reporting requests, and other system administration responsibilities.
Agency Administrator	Access project-level, client level, and agency user data	This role will grant the ability to view and edit data within the users' visibility settings, as well as basic project and end-user information.
Case Manager II & III	Access client-level data	This role will grant the ability to view and edit client-level data within the users' visibility settings.

Read Only	Access client-level data	This role will grant the ability to view client-level data within the users' visibility settings.

Passwords

Participating Agency HMIS end-users shall be issued a unique username and password. Default passwords must be changed upon initial log-in; passwords must have required rotation period and format enforcement, and must be 8-50 characters long with at least two numbers or symbols. Participating Agency end-users shall not compose passwords consisting of:

- Participating Agency end-user's own user ID;
- Proper names such as the Participating Agency end-user, application, or vendor name;
- Solely words from any dictionary; or
- Personally identifiable numbers such as phone extension, SSN, or zip code.

Passwords shall not be shared. Writing down passwords is only permitted if it can be stored where no one else, including managers and supervisors, can see or access it. Written passwords shall not also reference the user ID, the system, or the account where the data is stored.

5.3 Data/Information Classification and Handling, Collection, Maintenance, Assistance, and System Availability

Policy

This Policy and Procedures is to standardize expectations and provide guidance to Participating Agencies on the data entered into the HMIS, in order for the CoC to draw data-driven conclusions about and report on homelessness, the impact of homeless services, and other social issues affecting the San Diego region.

Procedure

All projects receiving Continuum of Care (CoC), Emergency Shelter Grant (ESG), and other federal funding sources outlined in the most recently published HMIS Data Standards Manual are contractually required to participate in the HMIS and must comply with expectations outlined by federal funding sources.

The HMIS Lead Agency is responsible for ensuring the HMIS is operated in accordance with HMIS Data and Technical standards. The HMIS Lead Agency is responsible for monitoring the HMIS to ensure projects are in compliance with the standards been set forth in these Policies and Procedures. The HMIS Lead Agency will work with Participating Agencies on ensuring compliance with the Policies and Procedures, and will demonstrate a reasonable level of discretion and will not make automatic determinations of agencies and/or projects being out of compliance.

The HMIS Lead Agency shall provide statistics and outcome measures for reports to the U.S. Department of Housing and Urban Development (HUD) and the Governance Board. The HMIS Lead Agency may produce HUD and Federal Partner required reports, such as the Housing Inventory Chart (HIC), the Annual Point in Time Count (PITC), and the Annual Homeless Assessment Report (AHAR).

The HMIS Lead Agency shall maintain a listing of all beds and service projects participating in HMIS and provide reports as required by the DAC.

The CoC, through the HMIS Lead Agency, retains the right to conduct site visits to check compliance with Privacy and Security Policies and Procedures and verify self-certification of Participating Agencies.

Media Sanitization and Reuse

Proper disposal of electronic and hard copy information in accordance with the following:

- When disposing of media (e.g., servers, workstations, mobile devices, and removable storage) which contain HMIS information, options include:
    - Final disposition of hardware, such as disk drives, shall be sanitized through crushing, shredding, incineration, or melting;
    - Use of a Certified Destruction Vendor.
- Hardware, such as desktop computers and servers, for reuse shall be sanitized by utilizing the DOD 5220.22-M standard.

Data Availability

The HMIS Lead Agency shall make every effort to have the HMIS available to Participating Agency end-users 98% of the year.

The HMIS Lead Agency shall inform end-users as soon as reasonable of any interruption in service.

Internet connection, a requirement of HMIS participation, is the sole responsibility of the Participating Agency.

The HMIS Vendor shall be required contractually to communicate with the HMIS Lead Agency any necessary downtime for system upgrades and patches.

- In the event it is determined that HMIS accessibility is disabled system-wide, the HMIS Lead Agency will work closely with the HMIS Vendor to resolve any issues;
- The HMIS Lead Agency shall email, or use other expedient means, to communicate disruptions of the HMIS to the Participating Agency Administrators within two (2) hours of problem awareness and provide an estimated time of system availability.

Access to information must be in timely manner, including temporary disruptions of business services or regional catastrophic interruption of services.

- The HMIS Lead Agency will grant access to information in relation to the HMIS' and the referring Participating Agency's business need via the process outlined in Access Controls;
- The HMIS Lead Agency shall develop, test, and implement a Contingency Plan and a Disaster Recovery Plan for operations to address interruption of HMIS services.

Maintenance and Disposal

The HMIS Lead Agency Executive Director (or other empowered officer) will be responsible for the maintenance and disposal of HMIS Lead Agency onsite computer equipment. This includes:

- Purchase of, and upgrades to, all computer equipment;
- HMIS Lead Agency systems credential issuance for workstations accessing HMIS including:
    - Unique username/password for operating system;
    - Enforcement of electronic controls such as auto-time out and password-protected screen saver.

All workstations and computer hardware (including Participating Agency network equipment) must be stored in a secure location (locked office area).

Retention

HMIS client data must be maintained for a minimum of seven (7) years. HMIS information may be kept for a longer period by the HMIS Lead Agency if required to do so by an applicable statute, regulation, contract or other requirement.

The HMIS Lead Agency may dispose of or anonymize information:

- Not accessed in the previous seven (7) years;
- Seven (7) years since last changed or amended.
- Anonymized information may be retained in alignment with the purposeful life of the information.

The HMIS Lead Agency shall coordinate with the HMIS Vendor to ensure data is retained and/or disposed of according to HMIS Policies and Procedures.

5.4 Privacy Use and Disclosures

Privacy Use and Disclosures Policy

In order to properly fulfill the responsibilities as the HMIS Lead Agency, all persons who have access to data must be informed on how they must, may, and may not, use or disclose information.

Procedure

The HMIS Lead Agency will list and define all uses and disclosures it performs via its Notice of Privacy Practices (NPP) (Appendix D).

The HMIS Lead Agency and staff have access to retrieve all data in the HMIS, however, the HMIS Lead Agency will protect client confidentiality in all reporting by limiting it to the minimum necessary to accomplish the reporting purpose.

The following data elements shall be collected by Participating Agencies and made available to those Participating Agencies who share common clients. The default minimum elements are:

- Client Profile;
- Universal Data Elements (UDEs) as outlined in the most recently published HMIS Data Standards;
- Program Specific Data Elements (PSDEs) as outlined in the most recently published HMIS Data Standards;
- Coordinated Entry System (CES) assessments including Vulnerability Index and Service Prioritization Decision Assistance Tool (VI-SDPAT) assessment and score (when applicable)
- File Attachments needed for coordinated assessment and housing placement;
- Program Case Manager and Contact Information; and
- Program Entry and Program Exit.

Participating Agencies who are also sub-recipients of federal funds shall comply with federal Title VI requirements as they apply to language accessibility.

Participating Agencies may use data they collect for any legal purpose, however, data accessed through the HMIS may only be used or disclosed for the purpose of coordination of client housing and services.

Entities providing funding to Participating Agencies, or projects required to use HMIS, will not have automatic access to the HMIS.

- Access to HMIS will only be granted according to the Access Controls;
- Funders requesting access to HMIS data, or summary reports, must submit through their contracted Participating Agency;

Any requests for reports or information from an individual or group who have not been explicitly granted access to the HMIS will be directed to the HMIS Lead Agency.

- No individual client data will be provided to meet these requests without DAC review of the data request.

Verbal Consent for Services

In an effort to more efficiently serve the client, the HMIS Lead Agency may authorize the use of a verbal process for assessment and documentation by 2-1-1 San Diego. The verbal process does not replace in person enrollment.

- The verbal process to collect information shall replace a written signature on the Multiparty Authorization (MPA) with a telephonic signature which will allow for authorized access to the client's data, and shall collect relevant identifiers to ensure unique identification of the individual and record of the Authorization;
- Authorized Participating Agencies shall certify in the HMIS they have talked to the individual, and to the best of their ability, collected the required unique identifiers and have indicated such by including a telephone reference number on the electronic file in the HMIS;
- "Data Not Collected" for identifier fields shall require physical corroboration prior to delivery of services;
- Verbal Consent process shall be monitored on an ongoing basis and should be used sparingly when a written signature is not possible;
- The HMIS Lead Agency must provide written authorization to Participating Agencies wishing to use the verbal consent process.

Research Projects

Request for research projects must be approved by the HMIS Lead Agency. Should the HMIS Lead Agency determine that additional review is required, the request will be forwarded to the DAC for a final determination.

Research that is approved by the Institutional Review Board (IRB) must meet the Office for Human Research Protections (OHRP) requirements for use of individual client data. Waiver of Informed Consent by an IRB does not constitute a waiver of individual privacy rights under other federal or state laws.

Requirement of an IRB for research is exempt at 45 CFR 46.101 where:

- Unless otherwise required by the research entity or Participating Agency heads, research activities in which the only involvement of human subjects will be in one or more of the following categories are exempt from this policy:
    - Research and demonstration projects which are conducted by or subject to the approval of the research entity or Participating Agency, and which are designed to study, evaluate, or otherwise examine:

- Public benefit or service programs;
- Procedures for obtaining benefits or services under those programs;
- Possible changes in or alternatives to those programs or procedures; or
- Possible changes in methods or levels of payment for benefits or services under those programs.

Access to client-level data for uses or disclosures not described here must be done only utilizing the Multiparty Authorization.

HMIS Reporting and Publication

The HMIS Lead Agency may utilize data in the HMIS for federal reporting, local evaluation, analysis, and publication.

To foster full transparency, identifiable project-level data pertaining to CoC and/or federally, state, or locally funded program performance may be published by the HMIS Lead Agency upon request by the Governance Board, Full Membership, and/or its subcommittees. Identifiable client-level data may only be released within the HMIS with client Authorization solely for coordination of housing and services. Clients may authorize the HMIS to release their information outside of the HMIS (ex.: Community Information Exchange (CIE)).

Participating Agency Procedure

Notification

At minimum, the HMIS Lead Agency requires Participating Agencies to post signs (Appendix F) where data collection occurs. The sign will include the following language:

"We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information as mandated by law or as requested from entities that fund this program. Other personal information we collect is necessary to operate programs, improve services, and better understand homelessness. We collect appropriate information only. A Privacy Notice is available upon request."

Participating Agencies must notify individuals seeking their assistance of data collection, use, and that disclosure will occur for the purposes of:

- Coordination of individual referrals, case management, housing, or other services; and
- Sharing with other organizations that may have separate privacy policies and that may allow different uses and disclosures of the information.

Data Standard Compliance

Participating Agencies and the HMIS Lead Agency are jointly responsible for ensuring project data in the HMIS meets the thresholds outlined in this policy:

- Participating Agencies will develop and implement a policy and procedure requiring that all client data be entered into the HMIS at point of service or within three (3) business days of a client interaction;
- Data required to be collected at entry and/or exit according to the most recently published HMIS Data Standards will be entered at point of service or within three (3) business days of a client's entry or exit date;
- Data required to be collected at least once every three (3) months or annually during program participation at least annually during enrollment, according to the most recently

published HMIS Data Standards, will be entered at point of service or within three (3) business days of the client reaching those respective deadlines;

- Data required to be collected at every contact or service provision according to the most recently published HMIS Data Standards will be entered at point of service or within three (3) business days of the contact/service.

The HMIS Lead Agency assumes that client information in the HMIS has been entered with the consent of the client through the Multiparty Authorization (Appendix C) process and in accordance with these HMIS Policies and Procedures. Participating Agencies shall maintain copies of the signed Multiparty Authorization.

Updates and Corrections Requests

Client requests to update information in the HMIS shall come from the Participating Agency.

If a Participating Agency agrees the information is inaccurate or incomplete, they may delete it or they may choose to mark it as inaccurate or incomplete and to supplement it with additional information.

Such corrections applicable to the data stored in the HMIS will be corrected within five (5) days of the determination that the request is accepted.

Clients who request to view data in the HMIS shall be documented by the Participating Agency.

- Agency Administrators or Case Managers may provide a copy of the requested data within a reasonable timeframe to the client;
- Participating Agencies with medical information are legally limited in establishing reasons for denying client requests for inspection of HMIS records and must, if applicable, follow either:
  - 45 CFR 164.524(d)(i through iii); or
  - Health & Safety Code 123.115(d).
- Partial releases may be permitted where the record contains information about another client or individual (other than a healthcare provider or homeless provider) and the denial is limited to the section of the record containing such information;
- Participating Agencies, after investigation, may reject repeated or harassing requests for access to or correction of an HMIS record;
- Participating Agencies who deny requests for access or correction will document the request and the reason for the denial.

The HMIS Lead Agency must ensure that Participating Agencies seek Authorization from the client prior to releasing client level HMIS data that do not fall within the scope of the purposes listed above.

Participating Agencies may only disclose HMIS data for the specific purposes and reasons defined on the Authorization form.

Participating Agencies may retrieve HMIS data entered to produce statistical reports for internal purposes and other required reports within the parameters established by the HMIS Lead Agency.

HMIS data download should be limited to the minimum necessary to accomplish the purpose.