

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

Policies and Procedures

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



March 31, 2020

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
3.2 Monitoring and Auditing	12

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	17
4.5 Maintenance of Onsite Computer Equipment	18
4.6 HMIS Technical Support Protocol	18
4.7 System Availability	19
4.8 HMIS Participation Fees	19
4.9 Training, Ethics, and Sanctions	19
5. Privacy and Security	
5.1 Privacy and Security	22
5.2 Role Based Access	25
5.3 Data/Information Classification and Handling, Collection, Maintenance, Assistance, and System Availability.....	26
5.4 Privacy Use and Disclosures	28

Appendices

- Appendix A:** Agency Participation Agreement
- Appendix B:** Multiparty Authorization to Use and/or Disclose Information
- Appendix C:** HMIS User Agreement
- 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

1. PROJECT SUMMARY

1.1 Background

Our vision is that homelessness in San Diego would be rare, brief and non-recurring. In order to accomplish our vision, we must know the scope of the problem, know the characteristics of those who find themselves homeless, and understand which homeless resolution strategies are effective and which are not. Reliable data enables our community to work confidently towards our goals as we 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 Longitudinal Systems Analysis (LSA) report, produced from a CoC's HMIS and submitted annually to HUD, provides HUD and Continuums of Care (CoCs) with critical information about how people experiencing homelessness use their system of care. 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, overseeing HMIS rules and regulations, and reporting 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 December 2019.

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 may 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 City and County CoC (CA - 601).

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 Clarity Human Services ("Clarity") a web-based HMIS software owned by Bitfocus, Inc., ("Bitfocus") 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 Bitfocus for this software and supports end-users with help desk, ongoing training, and project customization. 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 Bitfocus.

Clarity features:

- Combine the ease of the internet and the performance of a powerful database;
- Protects client confidentiality by carefully restricting access;
- Has 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.

2. HMIS LEAD AGENCY MISSION AND CONTACT INFORMATION

2.1 Regional Task Force on the Homeless (RTFH)

RTFH Mission

“RTFH is the homeless policy expert and lead coordinator for the introduction of new models and implementation of best practices for the San Diego Region.”

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@rtfhdsd.org
 Website: rtfhdsd.org

Role	Function
<i>Executive Director</i>	<ul style="list-style-type: none"> • CoC HMIS Lead Agency • HMIS direction & oversight
<i>HMIS System Administrator</i>	<ul style="list-style-type: none"> • General HMIS administration • Oversight and supervision of HMIS Technical Team
<i>HMIS Security Officer</i>	<ul style="list-style-type: none"> • Monitor security of the HMIS • Ensure HMIS Lead Agency and Participating Agency compliance with Security Policies and Procedures
HMIS Technical Team	
<i>HMIS Support Specialist</i>	<ul style="list-style-type: none"> • General technical support for HMIS issues related to end-user access, troubleshooting, information requests, system functionality errors, etc. • End-user training • Project setup and support • On boarding
<i>HMIS Data Analyst</i>	<ul style="list-style-type: none"> • 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 Evaluations Committee. The Evaluations Committee 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.

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 Evaluations Committee;
 - 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 Evaluations Committee;
- 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 Evaluations Committee 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 C);
- 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 Evaluations Committee 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 Evaluations Committee, 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 Evaluations Committee 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 Evaluations Committee;
- 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 Evaluations Committee 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 Evaluations Committee;
- The Evaluations Committee may sanction the Participating Agency, including revocation of access to the HMIS and CoC funding for that year, until such time as the Evaluations Committee determines the Participating Agency has achieved compliance. The Evaluations Committee 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 C).

Procedure

The HMIS System Administrator shall provide end-users authorized by Participating Agencies with an HMIS User Agreement (Appendix C) 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, and meet a data quality benchmark of < 5% error on all data collected.

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 Evaluations Committee and/or Governance Board provide project-level monitoring reports to the, 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

The most up to date version of the following web browsers is supported by Clarity:

- Microsoft Internet Explorer
- Microsoft Edge
- Google Chrome
- Apple Safari

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. RTFH offices are closed every other Friday. (Please see calendar at rtfh.org for Friday availability);
- 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

Standard arrangements should allow for continuous access to HMIS twenty-four hours a day for seven (“7”) days a week. 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). All HMIS licensing fees are subject to change.

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		
<i>HMIS 101</i>	Review of HMIS background and HMIS Data and Technical Standards	All new Participating Agency end-users, one time.
<i>HMIS Privacy, Security, and Ethics</i>	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.
Other Trainings		
<i>HMIS Refresher</i>	Workflow-specific review of navigating and using the HMIS, review of HMIS Data and Technical Standards	All existing Participating Agency end-users, annually.

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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ Mental Health or Alcohol Drug information; ○ HIV test results; and ○ 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 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	Description
<i>System Administrator</i>	Includes Enterprise and Manager level access and operation with the addition of System Administration management functions.
<i>Agency Manager</i>	Includes Enterprise level access and operation, with the addition of ability to customize agency preferences, including services and programs of the selected agency. Agency Manager license is required to run Data Analysis Tool.
<i>Enterprise (Agency Staff)</i>	Includes access and operation at the Enterprise level per each seat.

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 Solutions 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 Count (HIC), the Annual Point in Time Count (PITC), and the Longitudinal Systems Analysis (LSA).

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

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 Evaluations Committee 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 Evaluations Committee 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 B) 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.

HMIS Policies and Procedures:

Appendix



San Diego County CoC Homeless Management Information System (HMIS) Agency Participation Agreement

I. Purpose

The San Diego County Homeless Management Information System (HMIS) is a web-enabled database used by homeless service providers within the San Diego region to capture information about the persons they serve.

II. Audience and Agreement

This Agency Participation Agreement (“Agreement”) permits the Participating Agency listed below and its users to access the HMIS on their computer system through an Internet connection. The Participating Agency is the “Agency” named in this agreement as participants of the HMIS. The HMIS “Users” are the guardians entrusted with personal data to be entered and used in the HMIS and the “Client” is the consumer of services. The HMIS Lead Agency serves as the “System Administrator” whose primary function is to manage the HMIS.

All agencies which are granted access to the HMIS must agree to abide by all laws, and the HMIS Policies and Procedures pertaining to client confidentiality, user conduct, security, and the ongoing functionality and stability of services and equipment used to support the HMIS. Fees for HMIS use are outlined as Attachment A to this agreement.

The signature of the Executive Director or authorized designee of the Participating Agency indicates agreement with the terms set forth for an HMIS account for the Agency.

III. Confidentiality and Informed Consent

The Agency agrees to abide by and uphold all privacy protection standards established by the HMIS as well as their respective agency’s privacy procedures. The Agency will also uphold relevant Federal and California State confidentiality regulations and laws that protect client records, and the Agency will only release confidential client records with written consent by the client, or the client’s guardian, unless otherwise provided for in the regulations or laws. Access to the HMIS is granted to the Participating Agency based on the following premises:

Oral Explanation: All clients will be provided an oral explanation stating their information will be entered into a computerized record keeping system. The Agency will provide an oral explanation of the HMIS and the terms of consent. The Agency is responsible for ensuring that this procedure takes place prior to every client interview.

Written Explanation: Each client whose information is being shared with another Participating Agency must agree via execution of the Multiparty Authorization form. A Client must be informed as to what information is being shared and with whom it is being shared.

Information Release: The Agency agrees not to release client identifiable information to any other organization that is not listed on the Multiparty Authorization form without proper client consent except as provided by federal and California State law. See Multiparty Authorization (Appendix B) and Legal Citations (Appendix I). Releasing information to another HMIS Participating Agency shall not constitute an unauthorized disclosure, even in the event that no authorization form is on file.

Regulations: The Agency will uphold all relevant Federal and California State confidentiality regulations to protect client records and privacy. In addition, the Agency will only release client records with written consent by the client, unless otherwise provided for in the regulations. Specifically, but not limited to, the following:

- a. The Agency will abide specifically by the federal confidentiality rules as contained in the Code of Federal Regulations (CFR) 42 Part 2 Confidentiality of Alcohol and Drug Abuse Patient Records, regarding disclosure of alcohol and/or drug abuse records. In general terms, the Federal regulation prohibits the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by CFR 42 Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Agency understands that the Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.
- b. The Agency will abide specifically with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and corresponding regulations passed by the U.S. Department of Health and Human Services. In general, the regulations provide consumers with new rights to control the release of medical information, including advance consent for most disclosures of health information excluding treatment, the right to see a copy of health records, the right to request a correction to health records, the right to obtain documentation of disclosures of information may be used or disclosed. The current regulation provides protection for paper, oral, and electronic information.
- c. The Agency will abide specifically with the California Government Code 11015.5, and if applicable, CA Civil Code 1798, regarding Personal Information Collected on the Internet. In general, the Government Code ensures that any

San Diego County CoC Homeless Management Information System (HMIS) Agency Participation Agreement

electronically collected personal information about clients cannot be shared with any third party without the client's written consent.

Postings: Privacy and Mandatory Collection notices (Appendices E and F) must be posted at the Agency.

- A. The Agency must post Privacy and Mandatory Collection notices at each intake desk or comparable location.
- B. Privacy and Mandatory Collection notices must be made available in writing at the client's request.
- C. If the Agency maintains a website, a link to the privacy notice must be accessible from the Agency's website.

IV. Data Use

Data contained in the HMIS will only be used to support the delivery of homeless services in the San Diego region. Each User will affirm the principles of ethical data use and client confidentiality as noted and contained in the HMIS User Agreement.

1. The Agency will not solicit or input information from clients unless it is essential to provide services, or conduct program evaluation.
2. The Agency understands that all client data will be maintained on a central server, which will contain all client information in an encrypted state. All client identifiable data is inaccessible to unauthorized users.
3. The Agency shall use the system to enter and corroborate services but not for location services for past due billing.
4. The Agency shall not be denied access to client data entered by the Agency. Agencies are bound by all restrictions placed upon the data by the client of any Participating Agency. The Agency shall diligently record in the HMIS all restrictions requested.
5. The Agency shall not knowingly enter false or misleading data under any circumstances.
6. The Agency shall maintain appropriate documentation of client consent to participate in the HMIS.
7. If a client withdraws consent for release of information, the Agency remains responsible to ensure that the client's information is unavailable to all other Agencies.
8. The Agency shall keep signed copies of the Multiparty Authorization form for a period of seven (7) years.

V. Responsibilities

The Agency is responsible for ensuring that its staff does not intentionally or unintentionally misuse the HMIS. Such misuses are but are not limited to: damage of computing resources, obtaining unauthorized resources, taking resources from another user, gaining unauthorized access to resources, or otherwise using of computing resources without proper authorization.

1. The Agency will maintain an environment free of illegal or malicious acts and the Agency's users agree to never use the system to perform an illegal or malicious act. Any attempt to increase the level of access to which the User is authorized or any attempt to deprive other authorized Users of resources or access to HMIS shall be regarded as a violation of this Agreement that will be addressed as set forth in the HMIS Policies and Procedures.
2. Any User who finds a possible security lapse on the system is obligated to report it to the HMIS System Administrator immediately.
3. The HMIS software application was paid for with U.S. Department of Housing and Urban Development (HUD) grant funds. The maintenance, upgrades and license purchases are limited by the sanctions of the HUD grant.

VI. System Usage

Computer Equipment and Services are intended for HMIS-related activities. Acceptable computer system use includes data intake, reports, research of Client, Client development, and public service purposes. Prohibited Usage includes, but is not limited to, the following activities: the sending of fraudulent, threatening, harassing, or obscene messages and/or materials; inappropriate mass mailing (spamming, flooding, bombing); creation or intentional distribution of computer viruses, worms, or Trojan horses; unauthorized access to or denial of service; attempted attacks on any computer system.. Abusers are subject to sanctions as outlined in the HMIS Policies and Procedures.

VII. Rights

The HMIS Lead Agency reserves all rights, including access audit, termination of agreements, of the HMIS application and the service resources that it owns and/or operates on behalf of the Continuum of Care. These procedures shall not be construed as a waiver of any rights of the HMIS Lead Agency or the Participating Agency, nor shall they conflict with applicable acts of law.

San Diego County CoC Homeless Management Information System (HMIS)
Agency Participation Agreement

VIII. Privileges

The HMIS services and or equipment are a privilege and are assigned and managed by the HMIS Lead or designee(s). The Agency is responsible for proper use of the system as outlined in Section VI.

IX. Confidentiality

Although technological and procedural securities have been reasonably exhausted by the HMIS Lead to ensure client data confidentiality, this HMIS is being used by a multitude of end users and is therefore subject to the diligence to which the Participating Agencies' staff protects client records.

The protections that the HMIS put in place to protect client confidentiality include compliance with HUD Data and Technical Standards Final Notice, institution of a mandated HMIS training program for all HMIS users, consistent application of Policies and Procedures, and signed Agency End-User Agreements.

X. Copyright

The HMIS is protected by copyright and is not to be copied, except as permitted by law or by contract with owner of the copyright. The number of copies and distribution of copies are to be managed by the HMIS Lead. Interference with measures used by copyright holders to protect copyrighted works is prohibited.

Agency users storing materials copyrighted by others on the systems or displaying the materials through web pages must comply with copyright laws and guidelines.

XI. Violations

An individual violating any of the guidelines outlined in this agreement will be reported immediately upon discovery. Such suspected violations will be confidentially reported to the HMIS Lead and or the designee of that agency in accordance with the HMIS Policies and Procedures

Agreement

I have read this HMIS Agency Participation Agreement and thoroughly understand that this technology is for HMIS purposes only and is to be used in accordance with the HMIS Policies and Procedures.

This Agreement is executed between the Participating Agency listed below and the Regional Task Force on the Homeless (RTFH) acting as the San Diego County HMIS Lead Agency and upon execution the Participating Agency will be given access to the HMIS. The Executive Director or Authorized Designees for each Agency will sign this agreement.

Participating Agency (Print)

HMIS Lead Agency (Print)

Signature – Authorized Representative

Signature - Authorized Representative

Name (Print)

Name (Print)

Date

Date

San Diego County CoC Homeless Management Information System (HMIS)
Agency Participation Agreement

**Regional Task Force on the Homeless
 HMIS Clarity User License Fee Structure**

Types of User Licenses

HMIS Participating Agencies can purchase two different types of licenses that their staff can use to access San Diego County's HMIS software, Clarity: the Enterprise user license and the Manager license.

- Enterprise User License:** The Enterprise User License is the standard Clarity user license that is assigned to all users who do not need access to a Manager license.
- Manager License:** The Clarity Manager license is a license that includes access to agency/program management features and Clarity's data analysis interface, Looker. One user per agency is required to be assigned a Manager license; by default the Manager license will be assigned to the agency's primary HMIS administrator. Additional Manager licenses may be purchased/assigned upon request by the agency.

Fee Structure for Clarity Licenses

Type of License	Fee Structure
Clarity Enterprise User License	<p>Initial Setup Fee: \$175/new user license</p> <p>Monthly access fee (to be billed on a quarterly basis): \$25/user license</p> <p>*All HMIS licensing fees are subject to change.</p>
Clarity Manager License	<p>Initial Setup Fee: \$250/new Manager license</p> <p>Monthly access fee (to be billed on a quarterly basis): \$55/Manager license</p> <p>*All HMIS licensing fees are subject to change.</p>

Data Quality Incentives

RTFH may provide data quality incentives in the form of HMIS fee discounts. These incentives are not fixed or regular and will be provided and announced on an ad hoc basis. Information on incentives will be shared with providers once confirmed for each billing cycle.

Waiver Policy Statement

Waiver (or reduction) of fees for hardship may be submitted to RTFH and may be granted upon review. Requests for waivers must be submitted prior to the start of the upcoming billing cycle, so by January 1st of the year a waiver is being requested for.

Fees for other Requests

Other requests, including but not limited to custom reporting, data export/import and data integration projects, will be considered on a case-by-case basis. Cost estimates will be developed based upon a statement of work for the requested project.

Payment Methods

Checks and money orders are the only acceptable payment methods for HMIS licensing fees.

Multiparty Authorization to Use and/or Disclose Information

**To Receive Coordinated Care, Referrals and Services,
Please Review and Sign this Authorization Form.**

ABOUT RTFH HMIS AND 2-1-1 San Diego CIE: The San Diego County Homeless Management Information System (HMIS) managed by Regional Task Force on the Homeless (RTFH) and the Community Information Exchange (CIE) managed by 2-1-1 San Diego are two separate databases that are used to provide referral services to social services agencies for individuals with healthcare, housing, food, transportation, financial, and other needs. This authorization will allow HMIS and 2-1-1 participating agencies to collect information from you and your care team to assess your needs and put you in touch with social services agencies (Participating Agencies) they work with. Information will be shared with those Participating Agencies that provide services that can address your needs to coordinate referrals and services, track your progress and evaluate our success, among other things.

We are committed to protect your information from unlawful disclosure. This Authorization permits a Participating Agency to re-disclose health information to another Participating Agency and the information may no longer be protected under applicable health privacy laws. However, even if the Participating Agency is not subject to health privacy laws, RTFH, 2-1-1 San Diego, and their Participating Agencies are still required to employ administrative, technical, and physical safeguards to protect all information collected under this Authorization and use and disclose information in accordance with federal and state law.

By signing this form I authorize and request the Regional Task Force on the Homeless (RTFH), 2-1-1 San Diego, and Participating Agencies that they may refer me to or who may already be providing me with services to collect, record, use, and share my personally identifiable health, financial, housing, employment, and other relevant information with each other in order to assess my healthcare, housing, financial, and other needs, and to coordinate my care and provide comprehensive services to me.

The types of information that may be collected, used, and shared pursuant to this authorization includes, without limitation, the following to be shared in both HMIS and CIE:

- **Identifying Information:** Name, age, date of birth, social security number, address, personal ID, race, ethnicity, gender, contact information and contact information for family members, spouse, and my personal representatives

Multiparty Authorization to Use and/or Disclose Information

- **Housing:** Current location, destination, period of homelessness, prior residence, and local assessment data related to housing
- **Financial:** Employer, employment status, income, and non-cash benefits
- **Military:** Veteran status
- **Health Information:** Health and disability conditions and health insurance
- **Sensitive Information:** Drug, alcohol, and substance abuse, AIDS and HIV status, disabling conditions, developmental disabilities, mental health, and domestic violence information

Right to Decline or Revoke: I understand that I have the right to decline to share data or to revoke previous Authorization to share at any time by completing the Decline/Revocation form found at <https://www.rtfhsd.org/what-we-do/homeless-management-information-system-hmis/> and sending it to RTFH at: support@rtfhsd.org or by mailing it to the Regional Task Force on the Homeless, 4699 Murphy Canyon Road, Suite 104, San Diego, CA 92123.

I also understand that I have the right to individually revoke my consent to share data within 2-1-1 San Diego CIE at any time by visiting <https://ciesandiego.org/revoke/>

Expiration/Renewal: Unless otherwise revoked, to the fullest extent allowed by law, this Authorization shall remain valid for seven (7) years from the Effective Date indicated below. This Authorization may be renewed with my written consent.

Other Rights: I understand that authorizing the disclosure of information is voluntary and I can refuse to sign. I do not need to sign this form to be assured of housing and/or health care treatment services or enrollment in a housing program or health plan. However, if this Authorization is required for RTFH, 2-1-1 San Diego, and the Participating Providers to provide coordinated referrals and services and if I do not sign this Authorization, then my receipt of housing or other services may be limited or delayed.

Right to a Copy of My Information: I understand that I may inspect or obtain a copy of the information to be used or disclosed from my providers.

Right to a Copy of this Authorization: I have right to receive a copy this Authorization.

Authorized Participating Agencies: The current list of Participating Agencies with whom RTFH and 2-1-1- San Diego may share my information will be posted on the RTFH website: <https://www.rtfhsd.org/what-we-do/homeless-management-information-system-hmis/> and on the 2-1-1 San Diego CIE website: <https://ciesandiego.org/partners/>.

Multiparty Authorization to Use and/or Disclose Information

Client Information

Client/Head of Household Name

Date of Birth

Mailing Address/Place of Stay

Phone Number

Email

Signature of Individual or Legal Representative

Client Signature

Client Name

Date

San Diego County CoC Homeless Management Information System (HMIS) User Agreement

First and Last Name	
Job Title	
E-mail Address	
Phone Number with Extension	
Agency	
HMIS Provider ID # and Project Name for my Default Provider	
Other HMIS Provider ID #'s and Project Names I need EDA access to	
<i>Please check with your supervisor for Provider ID # and Project Name information</i>	
Training Date	

Purpose

The HMIS recognizes the priority of client needs in the design and management of the HMIS. These needs include both the need to continually improve the quality of homeless and housing services with the goal of eliminating homelessness in San Diego County, and the need to vigilantly maintain client confidentiality, treating the personal data of our most vulnerable populations with respect and care.

As the guardians entrusted with this personal data, HMIS end-users have a moral and a legal obligation to ensure that the data they collect is being collected, accessed, and used appropriately. It is also the responsibility of each employee, volunteer, and any other person with access to the HMIS to ensure that client data is only used to the ends to which it was collected, the ends that have been made explicit to clients and are consistent with the mission of the HMIS, to use the HMIS to advance the provision of quality services for homeless person, improve data collection, and promote more responsive policies to end homelessness in San Diego County.

Proper user training, adherence to the HMIS Policies and Procedures, and a clear understanding of client confidentiality and HMIS user responsibility are vital to achieving these goals.

Client Confidentiality

- A Multiparty Authorization form must be signed by each client whose data is to be shared within the HMIS. Client authorization may be revoked by that client at any time through a written notice.
- No client may be denied services for failure to provide authorization for HMIS data collection. Clients have a right to inspect, copy and request changes in their HMIS records.
- HMIS end-users may not share HMIS client data with individuals or agencies that have not entered into an HMIS Agency Participation Agreement or obtained written permission from that client.
- Excluding information shared in the client profile, HMIS users may not share client data with any agency that is not specified without obtaining a written permission from the client.
- HMIS end-users will maintain HMIS data in such a way as to protect against revealing the identity of clients to unauthorized agencies, individuals or entities.
- Personal User Identification (User ID) and Passwords must be kept secure and are not to be shared.
- Confidential information obtained from the HMIS is to remain confidential, even if the individual's relationship with the participating agency changes or concludes.
- Misrepresentation of the client data by entering known or inaccurate information is prohibited. Any information that is not given by the client should be marked unknown.
- Discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex and sexual orientation are not permitted in the HMIS. Profanity and offensive language are not permitted in the HMIS.
- The HMIS is to be used for business purposes only. Transmission of material in violation of Federal or California State regulations or laws is prohibited and includes material that is copyrighted, and/or judged to be threatening or obscene. The HMIS will not be used to defraud the Federal, State, or local government or an individual entity or to conduct any illegal activity.
- Any HMIS end-user found to be in violation of the HMIS Policies and Procedures, or the points of client confidentiality in this User Agreement, will result in immediate suspension of access to the HMIS and may jeopardize your employment status with the participating agency.

San Diego County CoC Homeless Management Information System (HMIS) User Agreement

Ethics

These general principles form the ethical or professional standards of conduct necessary for access to HMIS. Each end-user shall adhere to the delivery of services with the highest standards of professionalism, integrity, and competence.

1. Treat both clients and fellow employees respectfully, fairly and honestly at all times.
2. 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.
3. Conduct duties in conformance with all company policies and procedures.
4. Create a work environment that promotes open and honest communications, and encourages raising ethical concerns without fear of retribution or retaliation.
5. Assume responsibility for knowing, understanding and having a practical working knowledge of the laws and regulations applicable to your job.

User Responsibilities

- I affirm I have received training in using the HMIS, which is valid for one (1) year. I must attend an HMIS User Refresher training annually.
- I must login to the HMIS within thirty (30) days of receiving training. If I do not login within thirty (30) days of receiving training, I will be required to attend another training.
- I have read and will abide by all policies and procedures in the HMIS Policies and Procedures Manual.
- I will maintain the confidentiality of client data in the HMIS as outlined above and in the HMIS Policies and Procedures Manual.
- I will only collect, enter and extract data in the HMIS relevant to the delivery of services to people in housing crisis in the San Diego County region. I agree to use the data within the HMIS only for the purposes of homeless service delivery.
- I understand that my User ID and Password are for my use only and must not be shared with anyone, and I agree to take all reasonable precautions in keeping my password physically secure.
- I agree to refrain from leaving my computer unattended while logged into the system and further agree to log out of the system before leaving my work area.
- I agree to properly protect and store in a secure location client specific hardcopy information printed from the HMIS.
- I agree to notify my Agency Administrator and/or HMIS System Administrator in the case where I suspect that the HMIS security has been compromised.
- I agree, to the best of my ability, to enter and maintain accurate information into the HMIS.

Failure to comply with the provisions of this User Agreement, including Client Confidentiality, Ethics, and Responsibilities, is grounds for immediate termination of access to the HMIS. The signature below indicates an agreement to comply with the client confidentiality and user responsibilities. There is no expiration date of this agreement. My signature indicates that I have read this User Agreement, I am aware of my responsibilities, agree to abide by these standards of ethical conduct, have had the opportunity to ask questions, and agree that when I am in doubt as to the right action, I will seek support and advice from my supervisor or management.

User's Name	
User Signature	
Date	

Official HMIS Lead Agency Use Only

<i>User ID Assigned</i>					
<i>Access Level</i>	<i>Case Manager II</i>		<i>Case Manager III</i>		<i>Agency Administrator</i>
<i>Settings & Permissions</i>	<i>SkanPoint</i>		<i>ShelterPoint</i>		<i>ART License</i>
<i>Notes</i>					

San Diego County CoC Homeless Management Information System (HMIS)
Notice of Privacy Practices

Effective Date: _____

THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

If you have any questions about this Notice, you may contact either your service provider, or:

Regional Task Force on the Homeless
4699 Murphy Canyon Rd., San Diego, CA 92123
858-292-7627

Your information is personal, and the Regional Task Force on the Homeless (RTFH) is committed to protecting it. Your information is also very important to our ability to provide you with quality services, and to comply with certain laws. This notice describes the privacy practices our employees and other personnel are required to follow in handling your information.

We are legally required to: Keep your information confidential, give you this notice of our legal duties and privacy practices with respect to your information, and comply with this notice.

CHANGES TO THIS NOTICE

We reserve the right to revise or change the terms of this Notice, and to apply those changes to our policies and procedures regarding your information. To obtain a copy of this notice you can either ask your treatment provider or any staff person, or go to the RTFH's web site at <http://www.rtfhsd.org/>.

HOW WE MAY USE AND DISCLOSE YOUR INFORMATION

For Housing: We create a record of your information including housing services you receive at our partner agencies. We need this record to provide you with quality services and to comply with certain legal requirements.

Your service team may use or disclose your information to other personnel who are involved in providing services for you. For example, a housing navigator may need to know disability information to provide appropriate housing resources. Your service team may share your information in order to coordinate the different things you need, such as referrals and services.

We also may use and disclose your information to people outside this agency who may be involved in your service coordination when you access services from our partner agencies.

We may use and disclose your information to contact you with a reminder that you have an appointment and you have the right to tell us how you want to receive appointment reminders. At your request, a form will be provided to you for that purpose.

We may use and disclose your information to recommend service options or alternatives that may be of interest to you. Additionally, we may use and disclose your information to tell you about health-related benefits or services that may be of interest to you for example, Medi-Cal eligibility or Social Security benefits. You have the right to refuse this information.

For Service Corroboration: We may use or disclose basic information about you so that you do not have to provide information more than once. This sharing, only when you access one of the participating agencies, can help avoid duplication of services and referrals that you are already receiving.

For RTFH Operations: We may use and disclose information about you for administrative operations. These uses and disclosures are necessary to run our agency and make sure that all of our clients receive quality

San Diego County CoC Homeless Management Information System (HMIS)

Notice of Privacy Practices

services. For example, we may use information to review our services and evaluate the performance of our staff in providing those services.

We may also combine information from our participating agencies to decide what additional services should be offered, what services are not needed, and whether certain new services might be effective.

We may also combine the information with information from other agencies to compare how we are doing and see where we can make improvements in the services we offer. We may de-identify your information so others may use it to study services delivery without learning who the specific clients are.

Unless you object, we may disclose your information to any other person identified by you who is involved in your services. Your objection must be in writing (at your request, a form will be provided to you for this purpose). We will not honor your objection in circumstances where doing so would expose you or someone else to danger.

In the event of a disaster we may disclose your information to a housing disaster relief agency.

USES AND DISCLOSURES THAT DO NOT REQUIRE YOUR AUTHORIZATION

Research: Under certain circumstances, we may use and disclose information about you for research purposes. For example, a research project may involve comparing your service levels and of all clients who received similar services. All research projects, however, are subject to a special approval process. This process evaluates a proposed research project and its use of information, trying to balance the research needs with clients' need for privacy of their information. Before we use or disclose information for research, the project will have been approved through a research approval process, but we may, however, disclose information about you to people preparing to conduct a research project, for example, to help them look for clients with specific needs, so long as the information they review does not leave our agency.

As Required By Law: We will use and disclose information when required to do so by federal or state law or regulation.

To Avert a Serious Threat to Health or Safety: We may use and disclose your information when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person.

Public Health Activities: We may disclose your information for public health activities such as to report the abuse or neglect of children, elders and dependent adults;

Abuse, Neglect or Domestic Violence: We may disclose your information when notifying the appropriate government authority if we believe you have been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.

Oversight Activities: We may disclose your information to a federal oversight agency, such as the Department of Housing and Urban Development, for activities authorized by law. These oversight activities are necessary for the government to monitor government service programs, and compliance with civil rights laws.

Court Orders and Subpoenas: If you are involved in a lawsuit or a dispute, we may disclose your information in response to a court or administrative order. We may also disclose your information in response to a subpoena, discovery request, or other lawful process by someone else involved in a dispute.

Law Enforcement: We may disclose your information if asked to do so by law enforcement officials in any of the following circumstances:

- In response to a court order, subpoena, warrant, summons or similar process;
- About the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;

San Diego County CoC Homeless Management Information System (HMIS)

Notice of Privacy Practices

- About a death we believe may be the result of criminal conduct;
- About criminal conduct at any of our facilities; or
- In emergency circumstances to report a crime; the location of the crime, the victim(s); or the identity, description or location of the person who committed the crime.

OTHER USES OF YOUR INFORMATION

Other uses and disclosures of your information not covered by this Notice or the laws that apply to us will be made only with your written authorization. If you provide us authorization to disclose your information, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your information for the reasons covered by the authorization, except that, we are unable to take back any disclosures we have already made when the authorization was in effect, and we are required to retain our records of the services that we provided to you.

YOUR RIGHTS REGARDING INFORMATION ABOUT YOU

Right to Inspect and Obtain Copies:

With certain exceptions, you have the right to inspect and obtain copies of your information from our records. To inspect and obtain copies of your information, you must submit a request in writing to your service provider where you received services. If you request a copy of your information, they may charge a fee for the costs of copying, mailing or other supplies associated with your request.

We may deny your request to inspect and obtain copies of parts of your information. If you are denied the right to inspect and obtain copies of your information in our records, you may appeal this decision and request that another services professional designated by the RTFH, who was not involved in your treatment review the denial. (At your request, a form will be provided to you for this request.)

Right to Request an Amendment: If you feel that your information in our records is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as we keep the information. To request an amendment, you must submit a request in writing to your service provider. In addition, you must tell your provider the reason for the amendment, and at which agency you want your request to apply to. Your request will become part of your record. (At your request, a form and a list of participating agencies will be provided to you for this purpose.)

Right to Request Restrictions:

You have the right to request that we follow additional, special restrictions when disclosing your information. We are not required to agree to your request. If we do agree, we will comply with your request unless the information is needed to provide you with emergency treatment as determined by a doctor. To request restrictions, you must make your request in writing to your service provider. In your request, you must tell us what information you want to limit, the type of limitation, and to whom you want the limitation to apply.

Right to Request Confidential Communications: You have the right to request that we communicate with you about appointments or other matters related to your services in a specific way or at a specific location. For example, you can ask that we only contact you at work, or by mail at a post office box. To request confidential communications, you must make your request in writing to your Agency case manager or the person in charge of your services. Your request must specify how or where you wish to be contacted.

Right to a Paper Copy of This Notice: You may ask us for a paper copy of this Notice at any time. Even if you have agreed to receive this Notice electronically, you are entitled to receive a paper copy of this Notice. To obtain a paper copy of this Notice, ask any staff person. You may also obtain a copy of this Notice at our website www.rtfhsd.org.

San Diego County CoC Homeless Management Information System (HMIS)

Notice of Privacy Practices

COMPLAINTS

You have the right to file a complaint if you believe that RTFH staff has not complied with the practices outlined in this Notice. All complaints must be submitted in writing. You will not be penalized in any way for filing a complaint.

If you believe your privacy rights have been violated, you may file a complaint with the RTFH.

To file a complaint with the RTFH, contact:
Regional Task Force on the Homeless
4699 Murphy Canyon Rd., San Diego, CA 92123
858-292-7627

To file a complaint with the State of California, contact:
www.privacy.ca.gov
866-785-9663
800-952-5210

ACKNOWLEDGEMENT OF RECEIPT

By signing this form, you acknowledge receipt of the HMIS Notice of Privacy Practices. Our Notice of Privacy Practices provides information about how we may use and disclose your protected information. We encourage you to read it in full.

Our Notice of Privacy Practices is subject to change. If we change our notice, you may obtain a copy of the revised notice by accessing our web site, <http://www.rtfhsd.org/> or by contacting any staff person involved in your services.

If you have any questions about our Notice of Privacy Practices, please contact:
Regional Task Force on the Homeless
4699 Murphy Canyon Rd., San Diego, CA 92123
858-292-7627

I acknowledge receipt of the HMIS Notice of Privacy Practices.

Client Signature

Client Name, Printed

Date

Inability to Obtain Acknowledgement

To be completed only if no signature is obtained. If it is not possible to obtain the client's acknowledgement, describe the good faith efforts made to obtain the client's acknowledgement, and the reasons why the acknowledgement was not obtained:

Staff Member's Signature

Staff Name and Title Printed

Date

San Diego County CoC Homeless Management Information System (HMIS)
Summary of Privacy Practices

**THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED
SHARED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.**

PLEASE READ IT CAREFULLY

Effective Date: _____

Our Duty to Safeguard Your Protected Information

_____ collects information about who uses our services. We will ask for your permission to enter the information we collect about you and your family into a computer program called the Homeless Management Information System (HMIS) for the use of housing and services. Although the HMIS helps us to keep track of your information, individually identifiable information about you is considered "Protected Information." We are required to protect the privacy of your identifying information and to give you notice about how, when and why we may use or disclose any information you may give us.

We are also required to follow the privacy practices described in this Notice, although _____ **reserves the right to change our privacy practices and the terms of this notice at any time.** You may request a copy of the notice from any agency that participates in the HMIS.

How We May Use and Share Your Information

We use and share collective information for a variety of reports. We have a limited right to include some of your information for reports on homelessness. Information that could be used to tell who you are will never be used for these reports. We will not turn your information over to a state, local, private, or national database without your consent. We must have your written consent to use or disclose your information unless the law permits or requires us to make the use or disclosure without your permission. **Please review the Client Consent to Share and/or Disclose Information for details. You must sign this form before we can use your information, but you do not have to sign the form in order to receive services.**

Your Rights Regarding Your Information

- ✓ You have the right to get services even if you choose **NOT** to participate in the HMIS. However, clients may be refused program entry for not meeting other agency eligibility criteria.
- ✓ You have the right to ask for information about who has seen your information.
- ✓ You have the right to see your information and change it, if it is not correct.
- ✓ You have the right to revoke your consent to release information at any time. Information regarding the Client Revocation of Consent to Release Information is available at www.rtfhsd.org.
- ✓ You have the right to file a Grievance (complaint) if you feel your rights have been violated. Information regarding this HMIS Grievance Procedure is available at www.rtfhsd.org.

San Diego County CoC
Homeless Management Information System (HMIS)

MANDATORY COLLECTION NOTICE

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.

APPENDIX G: Client Revocation of Multiparty Authorization to Use and/or Disclose Information
San Diego County CoC Homeless Management Information System (HMIS)
Client Revocation of Authorization to Release Information

I, _____, hereby revoke permission for this agency to share my personal information in the San Diego County CoC Homeless Management Information System (HMIS) and also revoke my permission to share my data to the Community Information Exchange (CIE).

I understand that my information will remain in HMIS as part of the non-identifying data collected on homeless services provided by the San Diego County Continuum of Care (CoC) and I understand that my information will only be used according to the procedures outlined in the RTFH's HMIS Notice of Privacy Practices document.

I understand that information that has already been entered will remain in the system. By canceling my agreement for sharing information within the HMIS, my personal information that has been saved will be restricted.

I further understand that this revocation of data sharing only applies to information within the HMIS. Any information which was shared or retained outside of HMIS is not affected by this revocation. By signing, I acknowledge and understand that this Client Revocation of Consent to Release Information applies only to the sharing of information within the HMIS from this day forward.

I also understand that the disclosure of my non-identifying information may be required in some instances which are outlined in the RTFH's HMIS Notice of Privacy Practices document.

The San Diego County CoC HMIS Lead Agency and this agency are hereby released from any legal responsibility or liability for the release, use or disclosure of information I previously authorized.

Client Name	Date of Birth	Social Security Number
Client Signature	Date	
Agency Staff	Agency Staff Signature	
Agency Name	Date	

San Diego County CoC Homeless Management Information System (HMIS)
How to File a Privacy Complaint

If you feel that a violation of your rights as an HMIS client has occurred, or if you disagree with a decision that has been made about your Protected HMIS Information, you may complete this form and submit to the HMIS Lead Agency, the Regional Taskforce on the Homeless. Please complete this form only after you have exhausted the grievance procedures for the agency providing you housing and/or services. **It is against the law for any agency to take retaliatory action against you if you file this grievance.** You can expect a response within 30 (thirty) days via the grievance method of your choice.

Grievances must be submitted in writing to:
Regional Taskforce on the Homeless
4699 Murphy Canyon Rd.
San Diego, CA 92123

Brief Description of grievance (what happened):

_____ Date(s) of offense(s)

_____ Name of Individual(s) who violated your rights

_____ Name of Agency(ies) who violated your rights

Your Contact Information

Your Name	
Phone Number and/or Email Address	
Mailing Address	
Today's Date	

HMIS Lead Agency Use Only

Response Date	
Recommendation to Agency	

**San Diego County CoC Homeless Management Information System (HMIS)
Policies and Procedures Legal Framework**

a.	Handwritten by the person who signs it or is in typeface no smaller than 14-point type. [Cal. Civil Code 56.11(a)]
b.	Authorization is not combined with any other document to form a compound authorization. [45 CFR 164.508(b)(3) Cal. Civil Code 56.11(b)]
c.	Provides a specific and meaningful description of the information to be disclosed, including specific records and service dates. [45 CFR 164.508(c)(1)(i), and 42 CFR 2.31(3) requires patient NAMES and what kind of information]
d.	A specific division is identified as the one authorized to disclose the medical record. [45 CFR 164.508(c)(1)(ii); Cal. Civil Code 56.11(e) and 42 CFR 2.31(1)]
e.	Provides the name or other specific identification of the person(s) or entity(ies) to whom disclosure can be made. [45 CFR 164.508(c)(1)(iii); Cal. Civil Code 56.11(f) and 42 CFR 2.31(2)]
f.	Provides a statement of the purpose, and limitations, of the requested disclosure (which may be “at the request of the client”), including any limitations on the use of the information. [45 CFR 164.508(c)(1)(iv); Cal. Civil Code 56.11(g) and 42 CFR 2.31(4)]
g.	Provides an expiration date or a valid expiration event when information may no longer be disclosed, AND the date has not passed nor has the expiration event occurred. [45 CFR 164.508(b)(2)(i), 45 CFR 164.508(c)(1)(v), Cal. Civil Code 56.11(h) and 42 CFR 23.1(7) and (9)]
h.	Signed and dated by client or client’s authorized personal representative. If signed by the authorized personal representative, a description of such representative’s authority to act for the client is provided. [45 CFR 164.508(c)(1)(vi), Cal. Civil Code 56.11(c) and 42 CFR 2.31(6)]
i.	Statement of client’s right to revoke the authorization, exceptions to this right, and a description of how to revoke (a reference to the same information in the Notice of Privacy Practices may be provided instead of the last two items). [45 CFR 164.508(c)(2)(i) and (a); Cal. Civil code 56.15 and 42 CFR 2.31(8)]
j.	Statement that treatment, payment, enrollment or eligibility for benefits in health care services or health plan may NOT be conditioned upon signing the authorization. [45 CFR 164.508(c)(2)(ii)(A)]
k.	Statement regarding the potential that the information disclosed pursuant to the authorization may be re-disclosed by the recipient and, if so, it may no longer be protected by a federal confidentiality law (i.e., HIPAA) if the recipient of the medical record is not subject to such federal confidentiality law. [45 CFR 164.508(c)(2)(iii)]
l.	Statement that person signing the authorization has the right to (or will receive) a copy of the authorization. [45 CFR 164.508(c)(4) and Cal. Civil Code 56.11(i)]

Policies and Procedures Revision History

Version Number	Date	Author/Owner	Description of Change
1.1	April 21, 2016	Regional Taskforce on the Homeless	Approval of HMIS Policies and Procedures by the Regional Continuum of Care Council Governance Board
1.1	October 10, 2016	Regional Taskforce on the Homeless	Addition of new agencies to HMIS Trust Network/Multiparty Authorization
1.1	November 3, 2016	Regional Taskforce on the Homeless	Addition of new agencies to HMIS Trust Network/Multiparty Authorization
1.1	December 10, 2016	Regional Taskforce on the Homeless	Addition of new agencies to HMIS Trust Network/Multiparty Authorization
1.1	September 1, 2017	Regional Taskforce on the Homeless	Addition of new agencies to HMIS Trust Network/Multiparty Authorization. Other changes made to MPA include clarifying language, extending the term, adding a section to collect client contact information, and making it available in Spanish and as a fillable PDF.
1.2	September 21, 2017	Regional Taskforce on the Homeless	Administrative changes to the Policies and Procedures Manual and appendices. Clarifying language added to Agency Participation Agreement.
1.3	January 27, 2020	Regional Taskforce on the Homeless	Administrative changes to the Policies and Procedures. Updating our previous HMIS Vendor, and other edits pertaining to this change.
1.3	January 27, 2020	Regional Taskforce on the Homeless	Administrative changes to the Policies and Procedures. Making edits pertaining to the most recent HMIS Data Standards (i.e. FY 2020 HMIS Data Standards Manual).
1.3	January 27, 2020	Regional Taskforce on the Homeless	Administrative changes to the Policies and Procedures. Making edits to the Table of Contents to include some missing sections, and updating titles.