



HMIS/CEP Committee Meeting

February 24, 2025

1:00 pm to 2:00 pm

Housing Conference Room

Redding, CA 96001

2/24/2025 - 1:00 pm to 2:00 pm

Zoom link

<https://us06web.zoom.us/j/8758078882pwd=5VVYngpYM3GFvENdVmsSbeap98OVtU.1>

Teleconference locations:

**Del Norte County Health and Human Services
455 K Street
Crescent City, CA 95531**

**Sierra County Behavioral Health
704 Mill Street
Loyalton, CA 96118**

**Teach I.N.C
112 E 2nd Street
Alturas, CA 96101**

**Lassen County Health and Social Services
1410 Chestnut Street
Susanville, CA 96130**

**Siskiyou County Behavioral Health
2060 Campus Dr.
Yreka, CA 96097**

**Plumas County
PCIRC
591 Main Street
Quincy, CA 95971**

**HMIS/CEP
Committee Members**

Maddelyn Bryan, Chair
County of Siskiyou

Kristen Quade, Vice Chair
County of Plumas

Carla McDonald,
County of Lassen

Daphne Cortese-Lambert,
County of Del Norte

Vacant,
County of Modoc

Robert Szopa,
County of Sierra

Sarah Prieto,
County of Shasta



To Address the Board: Members of the public may address the Board on any agenda item. Pursuant to the Brown Act (Govt. Code section 54950, et seq.) Board action or discussion cannot be taken on non-agenda matters but the board may briefly respond to statements or questions. You may submit your public comment via email to norcalcoc@cityofredding.org that will be read into the record.

1. Call to Order/Quorum Established/Introductions

2. Public Comments (limited to 3 mins. per comment)

Members of the public will have the opportunity to address the Board on any issue within the jurisdiction of the Board. Speakers will be limited to three minutes.

3. Action Items

I. Review and Approve updates the Security Section of the HMIS Policies and Procedures

Attachment A

II. Review and Approve updates to the Coordinated Entry Assessment required by HUD

Attachment B

4. Discussion

I. Data Quality benchmarks (Amanda)

5. Reports

I. HMIS Members

II. UWNC

6. Adjournment

If requested, the agenda shall be made available in appropriate alternative formats to persons with a disability, as required by Section 202 of the Americans with Disabilities Act of 1990 (42 U.S.C. Sec. 12132), and the federal rules and regulations adopted in implementation thereof. You may contact the City of Redding Housing Division at (530)225-4048 for disability-related modifications or accommodations, including auxiliary aids or services, in order to participate in the public meeting.

Next HMIS Meetings

March 17, 2025 1 pm – 2pm

Redding City Hall, Housing Conference Room

Next NorCal CoC Executive Board Meeting

March 20, 2025 1pm – 3pm

Redding City Hall, Enterprise Conference Room

NorCal CA 516
Homeless Continuum of Care

Homeless Management Information System (HMIS)
Policies & Procedures

March 2024

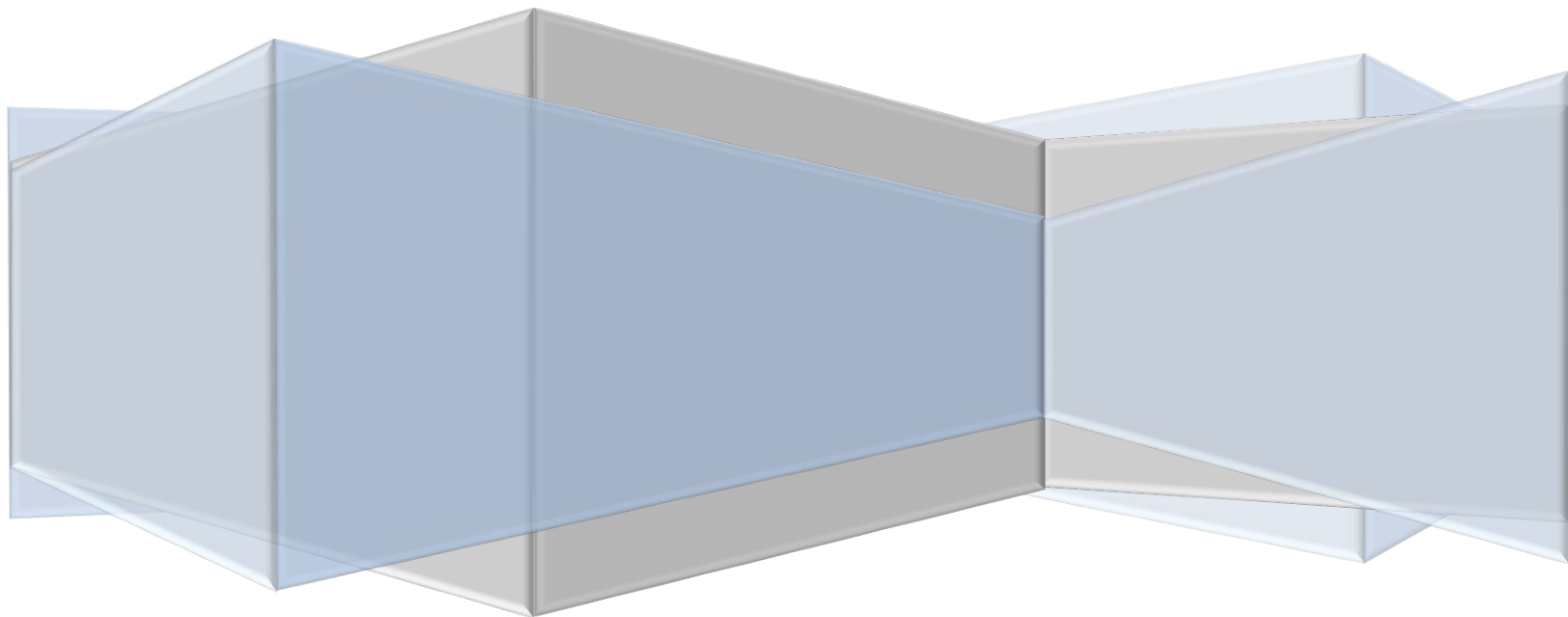


Table of Contents

1. PROJECT SUMMARY	3
1.1 Background	3
1.2 NorCal CA 516 Homeless Continuum of Care	3
1.3 HMIS Software	3
2. HMIS DEFINITIONS	4
3. CONTINUUM OF CARE STRUCTURE	5
4. STANDARDS FOR HMIS GOVERNANCE	6
4.1 HMIS Committee	6
4.2 Requests for Policy Addition, Deletion, or Change	6
4.3 Mandated Additions, Deletions, or Changes	7
5. HMIS DATA QUALITY STANDARDS	8
5.1 Applicability, Purpose and Goals	8
5.1.1 Data Quality Plan	8
5.1.2 Monitoring by System Administrator	8
5.2 Data Quality Benchmarks	9
5.2.1 Data Accuracy Benchmarks	9
5.2.2 Data Completeness Benchmarks	9
5.2.3 Data Timeliness Benchmarks	10
5.3 Data Completeness Required Reports	10
Description	10
5.4 Reduce Duplications in HMIS for Every Participating Agency	10
5.5 Data Quality and Correction	11
6. PRIVACY STANDARDS	12
6.1 Policies and Applications	12
6.1.1 Privacy Policy and Mandatory Collection Notice	12
6.1.2 Informed Consent Process	12
6.1.3 HMIS Client Consent Form – Release of Information (ROI)	13
6.2 Revoking Authorization for HMIS Data Collection	15
6.3 Client’s Access to Their Information	15
6.4 Client Grievance Process	15
6.5 Electronic Sharing of Client Data	16
7. SECURITY STANDARDS	17
7.1 Security Management	17
7.1.1 Security Plan	17
7.2 Workstation Security Procedures	17
7.3 HMIS Software Application – Level Security	18
7.4 Security Review	19
8. HMIS IMPLEMENTATION	20
8.1 HMIS Software Solution	20
8.2 Technology Requirements	20
8.3 Inter-Agency Data Sharing Agreement	21
8.4 End User Agreements	21
8.4.1 Removing Authorized Personnel	22
8.5 HMIS Licensing	22

8.6 Designate Participating Agency HMIS Lead.....	23
8.7 Participating Agency Profile in HMIS	23
8.8 Designating Participating Agency End Users	24
9. DATA COLLECTION & REPORTING	25
9.1 On Whom to Collect Data	25
9.2 Using Paper-based Data Collection Forms	25
9.3 Client Intake: Completing Required Fields in HMIS.....	26
9.5 Client Discharge: Exiting Clients from Programs.....	27
10. TRAINING & TECHNICAL ASSISTANCE.....	28
10.1 End User Training.....	28
10.2 Training Refresher.....	29
10.3 Contacting the System Administrator	29
Appendix A: HMIS Client Consent Form	30
Appendix B: Privacy Policy	35
Appendix C: Mandatory Collection Notice	39
Appendix D: HMIS Request for Policy Addition, Deletion, or Change	41
Appendix E: Inter-Agency Data Sharing Agreement	43
Appendix F: Revocation Form	46
Appendix G: Client HMIS Grievance Form.....	48
Appendix H: HMIS End User Agreement.....	50
Appendix I: Adult Intake Form.....	53
Appendix J: Minor Intake Form.....	58
Appendix K: Exit Form – all household members	60
Appendix L – Privacy and Security Plan	64

1. PROJECT SUMMARY

1.1 Background

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

A Homeless Management Information System (HMIS) is an information system designated by a local Continuum of Care (CoC) to comply with the requirements of CoC Program Interim Rule 24 CFR 578 (07/2012). It is a locally administered data system used to record and analyze client, service, and housing data for individuals and families who are experiencing homelessness or at risk of homelessness. HMIS is a valuable resource because of its capacity to integrate and de-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.

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

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

US Department of Housing and Urban Development has released a HMIS Data Standards Manual, (<https://files.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf>), which provides communities with baseline data collection requirements developed by each of these federal partners.

These Data Standards are designed for CoCs, HMIS Lead Agencies, HMIS System Administrators, and HMIS Users to help them understand the data elements that are required in HMIS to meet participation and reporting requirements, established by HUD and the federal partners. The latest Data Standards will be followed as released by HUD.

1.2 NorCal CA 516 Homeless Continuum of Care

The NorCal CA 516 Continuum of Care has designated United Way of Northern California (UWNC) to serve as the HMIS System Administrator. In that capacity, UWNC is responsible for the management and development of the NorCal CA 516 HMIS. Agencies with homeless-dedicated programs are highly encouraged to participate in HMIS to support local data collection, service, and planning functions in the NorCal CA 516 jurisdiction. NorCal CA 516 jurisdiction encompasses Del Norte, Lassen, Modoc, Plumas, Shasta, Sierra and Siskiyou Counties.

1.3 HMIS Software

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

The NorCal CA 516 CoC has selected WellSky's Community Services (ServicePoint), a web based HMIS software, to be the HMIS software of record. It empowers human service providers, agencies, coalitions, and communities to manage real-time client and services data. As the HMIS Lead Administrator, UWNC

has contracted directly with WellSky for HMIS software; supports end-users with a help desk; provides ongoing training; and customizes projects including development of project-specific assessments and settings. SCCAA works directly with Participating Agencies to identify needs and requirements for custom reports developed by SCCAA or canned reports made available by WellSky.

2. HMIS DEFINITIONS

Client: A living individual about whom a Participating Agency collects or maintains protected personal information: (1) because the individual is receiving, has received, may receive, or has inquired about services; or (2) in order to identify service needs, or to plan or develop appropriate services within the CoC.

Continuum of Care (CoC): The group organized to carry out the responsibilities and requirements under 24 CFR part 578 that is composed of representatives of organizations including: nonprofit homeless providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve homeless and formerly homeless veterans, and homeless and formerly homeless persons to the extent these groups are represented within the geographic area and are available to participate.

CoC Program: A program identified by the CoC as part of its services system, whose primary purpose is to meet the specific needs of people who are experiencing a housing crisis.

Contributory CoC Programs: A homeless assistance program or homelessness prevention program that contributes Protected Identifying Information or other client-level data to an HMIS.

Contributory Non-CoC Programs: A program that is neither a homeless assistance program nor a homelessness prevention program that contributes Protected Identifying Information or other client-level data to an HMIS.

HMIS System Administrator: An organization designated by a CoC to operate the CoC's HMIS on its behalf.

Homeless Management Information System (HMIS): The information system designated by NorCal CoC CA 516 and Dos Rios CoC CA 523 to comply with the requirements of HUD used to record, analyze, and transmit client and activity data in regard to the provision of shelter, housing, and services to individuals and families who are experiencing homelessness or at risk of homelessness.

HUD: United States Department of Housing and Urban Development.

Administrative Entity: An agency that the CoC has established to provide guidance to ensure that the duties of the CoC are being met.

Participating Agency: An organization that operates a project that contributes data to an HMIS.

Participating Agency HMIS Lead: An individual designated by the Participating Agency Executive Director, or other empowered officer, to act as the Participating Agency HMIS Lead.

The Participating Agency HMIS Lead is the liaison between the HMIS System Administrator and the Participating Agency's End Users.

Participating Agency End User: An employee, volunteer, affiliate, associate, and any other individual acting on behalf of a Participating Agency, who uses or enters data into HMIS.

Participating CoC Program: A contributory CoC Program that makes reasonable efforts to record all the universal data elements and all other required data elements as determined by HUD funding requirements on all clients served.

Protected Identifying Information (PII): Information about a Client that can be used to distinguish or trace a Client's identity, either alone or when combined with other personal or identifying information, using methods reasonably likely to be used, which is linkable to the Client.

Security Officer: An individual designated at each Participating Agency to be responsible for ensuring compliance with applicable security standards.

System Administrator: An individual designated by the HMIS System Administrator to act as the System Administrator. The System Administrator is the liaison between the Participating Agencies and the HMIS System Administrator .

Victim Services Provider: A nonprofit or nongovernmental organization including rape crisis centers, battered women's shelters, domestic violence transitional housing programs, and other programs whose primary mission is to provide services to victims/survivors of domestic violence, dating violence, sexual assault, or stalking.

3. CONTINUUM OF CARE STRUCTURE

NorCal CA 516 Continuum of Care (CoC) is comprised of public and private agencies along with community residents including homeless and formerly homeless individuals. The CoC is designed to assess the need for homeless and affordable housing services; and to develop and recommend a Continuum of Care Plan for the region on behalf of individuals and families at-risk of and experiencing homelessness.

4. STANDARDS FOR HMIS GOVERNANCE

4.1 HMIS Committee

Policy:

The HMIS/Coordinated Entry Process (CEP) Committee is made up of various members from the community. The NorCal CoC Executive Board will appoint at a minimum (1) committee member from each county and (1) alternate. Committee members are required to attend not less than 75% of scheduled meetings per year. The purpose of these meetings is to establish and enforce HMIS Policies and Procedures; Coordinated Entry Policies and Procedures assist in the planning of all point-in-time counts; review all participating agencies' compliance reports, review all requests for changes to the policies; and plan/participate in compliance monitoring. The HMIS Committee is actively involved in furthering CoC goals.

Description:

To ensure every Participating Agency is compliant with HUD and County mandated Policies and Procedures, it is necessary for each county in the Continuum of Care to be involved in the formulation of these Policies and Procedures. These meetings will give Participating Agencies the opportunity to voice their concerns as well as determine what and how the policies are written and enforced.

Procedures:

- The HMIS System Administrator will host, moderate, and determine where each quarterly meeting will take place.
- The HMIS System Administrator will post agendas 72 hours prior to the meeting and conduct the meeting in accordance with the Brown Act.
- Members wishing to add items to agendas can do so by emailing their requests at least one week prior to the meeting date to: HMIS@NorCalUnitedWay.org.
- Changes and additions to the policy manual require Committee approval. All requests for changes must be submitted on a Request for Policy Change or Addition Form (Appendix D) in order to be considered by the Committee.
- The HMIS System Administrator will distribute minutes of each meeting 72 hours before the next scheduled HMIS Committee Meeting.

Best Practice:

- Participating Agencies are strongly encouraged to suggest topics that they feel should be discussed.
- Participating Agencies are encouraged to share their ideas and best practices that they feel others in the community would benefit from as well.

4.2 Requests for Policy Addition, Deletion, or Change

Policy:

All requests for changes to the Policies & Procedures Manual must be made in writing and will be tracked by the HMIS System Administrator. Requests received will be reviewed by the HMIS Committee prior to being changed in the Policies and Procedures

Description:

All requests for changes to this Policies and Procedures Manual must be submitted in writing in order to be reviewed at the quarterly HMIS/CE Committee Meetings. All NorCal CA 516 CoC members are welcome to submit requests. Submitting a request does not guarantee approval of the request.

Procedure:

- Complete an HMIS Request for Policy Addition, Deletion, or Change (Appendix D) form and submit it to the HMIS System Administrator.

By mail:

United Way of Northern California
Attn: HMIS System Administrator
3300 Churn Creek Road
Redding, CA 96002

By Phone:

(530) 241-7521
Attn: HMIS System Administrator

By email:

HMIS@NorCalUnitedWay.org

- HMIS System Administrator will present changes to HMIS Committee for discussion and recommended action, which may include approval, denial, or other appropriate, reasonable determinations.
- Approved requests will be amended in this Policies and Procedures Manual and uploaded to the City of Redding's website under the NorCal Continuum of Care within 7 business days following approval.

4.3 Mandated Additions, Deletions, or Changes**Policy:**

All legislative, regulatory, or other legal authority changes to the Policies & Procedures Manual must be implemented within the time frame established by HUD.

Description:

Changes that are mandated by HUD will be implemented by the HMIS System Administrator in the designated time frame according to the HUD requirements.

Procedure:

- Upon notice from HUD of regulatory changes, the HMIS System Administrator will send out written notice to each Participating Agency.
 - At the next scheduled HMIS Committee Meeting, the HMIS System Administrator will present any HUD mandated changes.
 - All changes will be implemented within the time frame established by HUD and a new Policies and Procedures Manual will be published on the City of Redding's website under the NorCal Continuum of Care.
-

5. HMIS DATA QUALITY STANDARDS

5.1 Applicability, Purpose and Goals

The Data Quality Standards ensure the completeness, accuracy, and consistency of the data in HMIS. The Data Quality Standards and Management encompass the Data Quality Plan, Data Accuracy, Data Completeness, and Data Timeliness Benchmarks, Data Quality Reports and correction of data when necessary.

5.1.1 Data Quality Plan

Policy:

The HMIS System Administrator will implement this Data Quality Plan to ensure consistent data collection and data quality across all Participating Agencies.

Description:

At minimum the Data Quality Plan must include the following elements:

- Identify the responsibilities of all parties in the CoC (Executive and Advisory Boards, HMIS System Administrator, Participating Agencies, and Participating Agency End Users) with respect to achieving good quality HMIS data.
- Benchmarks for data timelessness, data accuracy, and data completeness.

5.1.2 Monitoring

Policy:

The HMIS System Administrator will monitor the overall data quality entered by individual Participating Agencies.

Description:

Specifically, the HMIS System Administrator will:

- Utilize the Data Quality Report and the Data Quality Detail Report to monitor data quality for each Participating Agency.
 - Review monthly program level information for each Participating Agency identifying data quality weaknesses and recommending solutions for issues that need to be addressed.
 - Provide regular feedback to individual Participating Agencies to ensure problems are addressed.
 - If after receiving technical assistance and assistance of the user's program manager, a licensed user who continues to have persistent data quality errors, access to the HMIS system will be deactivated until such time that the user attends additional training and/or technical assistance. The HMIS Administrator will notify the participating agency that the user will be deactivated.
 - Monitor the updating of Client data that has been identified as non-compliant with the Data Quality Plan.
-

5.2 Data Quality Benchmarks

5.2.1 Data Accuracy Benchmarks

Policy:

To qualify as “participating in the HMIS,” all Participating Agencies must meet the data quality benchmarks as described in the Data Quality Plan.

Description:

Client information entered must be valid and accurately represent information provided to End User. Every Participating Agency must enter data on Clients in the same way over time, regardless of which staff person is entering the data.

Procedure:

To determine the accuracy of information, Participating Agencies must regularly conduct data quality checks.

5.2.2 Data Completeness Benchmarks

Description:

All data entered should be complete. Partially complete or missing data can negatively affect the quality of data. Missing data could mean the client does not receive the services that could help them become permanently housed and end their homelessness.

Procedure:

The Participating Agency HMIS Lead should check the completeness of the data entered by Participating Agency End Users within their agency.

Required Benchmark:

100% of all HUD funded homeless assistance programs (excluding Victim Services Provider programs) must participate. The Data Quality Benchmark for participating projects is to maintain an overall average of 95% score from the Data Completeness Report for the agency.

5.2.3 Data Timeliness Benchmarks

Description:

To be most useful for reporting, the most up-to-date information possible on Clients must be included.

Procedure:

Client information must be entered by Participating Agencies within 5 business or 7 calendar days of the event (Intake/enrollment, service delivery, or exit). Every Participating Agency must update Client information at exit and/or at annual assessment, per the requirements relative to each Universal and Program Specific Data Element.

5.3 Data Completeness Required Reports

The overall standards for HMIS software are presented in the Homeless Management Information System (HMIS) Data and Technical Standards Final Notice as published by HUD (Vol. 69, No. 146, July 30, 2004). Copies are available upon request.

Description

This report calculates the percentage of required Client-level data elements with null or missing values divided by the total number of Client records. The report will also calculate the number of useable values (all values excluding “Don’t know” and “Refused” responses) in each required field over any desired time period (e.g., last month, last year). The report can be generated for each of the Participating Agencies’ programs. The program level reports will cover all applicable Universal and Program Specific Data Elements. Percentages will be based on the universe of client records for which the data element is required. For example, percent (%) null for veterans = number of clients with no veteran status recorded/number of adults.

5.4 Reduce Duplications in HMIS for Every Participating Agency

Policy:

To reduce the duplication of Client records, Participating Agency HMIS End Users should always search for the Client before creating a new Client record.

Description:

The burden of not creating duplicate records falls on each Participating Agency End User. The HMIS does not prevent the creation of duplicate Client records; therefore, it is up to each HMIS End User to ensure every Client is first searched for and if not found, added. If matches are found, the Participating Agency End User must determine if any of the records found match the Client for which they are entering data.

Procedures:

- When an End User is collecting data, the End User will first attempt to locate the Client by searching for them by first name, if not found, then, by last name; and if not found, a search by social security number (SSN) only.
- If no matches are found for the Client, the HMIS End User will continue to add the basic Universal Data Elements.

Best Practices:

The HMIS End User should perform more than one type of search when attempting to find an existing record. Clients often do not use the exact same name that was previously entered.

- Using a field other than “name” tends to be more accurate and not open for interpretation

5.5 Data Quality and Correction

Policy:

The Participating Agency HMIS Lead is required to run the Data Quality Report for each of the Participating Agency’s programs and respond to the HMIS System Administrator’s request for data clean-up.

Procedures:

- Based on the Data Reporting Schedule, the HMIS System Administrator will review the quality of each Participating Agency’s data.
 - Participating Agency HMIS Leads are required to run the required reports and work with the HMIS System Administrator to rectify any shortfalls on data quality within the outlined time frame on the Data Reporting Schedule.
-

6. PRIVACY STANDARDS

6.1 Policies and Applications

The HMIS System Administrator will provide to all Participating Agencies, and make otherwise publicly available to anyone upon request, notices that:

- Describe its role in the processing of Personally Identifiable Information obtained from Participating Agencies.
- Describe accountability measures for meeting applicable privacy and security obligations.
- Inform clients how to pursue their privacy rights with Participating Agencies.

6.1.1 Privacy Policy and Mandatory Collection Notice

Policy:

All Participating Agency End Users must have a sign posted at their workstation or wherever data is collected that describes how information about the client may be used and disclosed and how the client can get access to their information.

Description:

The Mandatory Collection Notice (Appendix C) must be posted at each workstation, desk, or area used for HMIS data collection. The HMIS Privacy Policy (Appendix B) is a document describing a client's data rights in relation to HMIS.

Procedures:

- Post the HMIS Mandatory Collection Notice at each workstation, desk, or area used for HMIS data collection.
- Upon request by a client, the HMIS Privacy Policy shall be provided.

Best Practice:

A Participating Agency could also post the HMIS Mandatory Collection Notice in a waiting room, an intake line, or another area where clients congregate before intake occurs. This will give clients another opportunity to read the notice before receiving services.

6.1.2 Informed Consent Process

Policy:

All clients must go through the Informed Consent Process.

Procedure:

Once a client has been determined eligible for services at a Participating Agency, a Participating Agency End User must verbally explain the use and benefits of HMIS using the Client Consent Form as a guide.

It is the responsibility of the user who is conducting the intake interview to determine if a current Release of Information is uploaded into the system.

Best Practice:

It is recommended that End Users go through the Informed Consent Process consistently with each client.

6.1.3 HMIS Client Consent Form – Release of Information (ROI)**Policy:**

All clients' HMIS Client Consent forms must be stored securely for a minimum of three years from date signed.

Procedures:

- The Client Consent Form – Release of Information (ROI) (Appendix A) is valid for three years from the date signed by Client. Therefore, for auditing purposes, it is important to keep the signed HMIS Client Consent form (ROI) for at least that length of time, unless the form is uploaded to HMIS.
- Client Consent forms (ROI) must be kept securely in accordance with standard confidentiality and privacy practices (e.g. locked away in a file cabinet and not accessible without authorization).
- If a Participating Agency does not currently keep client files, they must establish a file system to maintain Client Consent forms (ROI).
- If a Participating Agency chooses to upload each Client Consent form (ROI) into HMIS (preferred method), each Client Consent form (ROI) may be shredded.

Best Practices:

It is recommended that Participating Agencies keep the Client Consent form (ROI) in their current client file with the other information being collected and maintained. It will be easier to locate their information in this manner rather than creating a separate file for HMIS.

Policy:

Participating Agencies will give clients a copy of the HMIS Client Consent form- Release of Information (ROI).

Procedures:

- The Client Consent form (ROI) details the client's rights in HMIS data collection. This information is particularly important to those clients that agree to participate in HMIS.
- At the client's request, the Participating Agency End User should make a copy of the Client Consent form (ROI) and give it to the client.

Best Practice:

Participating Agencies should provide clients with a photocopy of the Client Consent form-Release of Information (ROI), so that the client has a record of their HMIS participation decision.

Policy:

If an end user determines that the client is unable to give consent, the end user will seek guidance from the program manager or the HMIS Administrator.

Procedures:

- The industry-wide best practice is to presume that all clients are competent, unless there is a known court ordering stating otherwise.
- If there is a known, current, and valid court order stating the individual is not competent, then it is not possible for that individual to provide a Client Consent Form. In this case, the HMIS End Users should mark down "DO NOT ENTER MY INFORMATION" and sign as the Participating Agency witness.

Policy:

The data in HMIS is owned by the NorCal CoC or the client owns their own personal data.

Procedures:

- If an outside entity wants aggregated data from the NorCal CoC HMIS database, a proposal that includes the intent and the audience for which the data will be presented must be submitted for approval by the NorCal CoC Executive Board.

Policy:

Clients **do not** have to participate and/or share their information in HMIS to be served by the program.

Procedures:

- A number of clients may choose not to participate and/or share their information in HMIS; however, it is important for reporting purposes that these individuals are still counted.
- To account for the overall services rendered by a Participating Agency, each Participating Agency must keep track of how many clients did not participate in HMIS.

Policy:

Participating Agencies **cannot** deny services to an individual solely on the basis of the individual deciding not to participate and/or share their information in HMIS.

Procedure:

- Participating Agencies must determine if an individual will or will not receive services before the individual goes through the Informed Consent process.
-

6.2 Revoking Authorization for HMIS Data Collection

Policy:

Clients who initially agree to participate and/or share their information in HMIS have the right to rescind their permission for data collection.

Procedures:

- In order to rescind his or her permission to participate and/or share information in HMIS, a client must request and complete the Revocation Form (Appendix F).
- The Participating Agency will file the completed Revocation Form with the client's previously signed Client Consent Form.
- The Participating Agency will promptly contact the HMIS System Administrator to request that the client's record visibility settings be restricted and not shared.

Best Practices:

If a client comes into a Participating Agency that never provided services to the client and requests a Revocation Form, the Participating Agency shall collect the completed Revocation Form and forward form to the HMIS System Administrator.

6.3 Client's Access to Their Information

Policy:

Clients have the right to a copy of their Universal and Program Specific data contained within HMIS.

Procedures:

- Clients may request a copy of their information contained within HMIS.
- Upon request of the client, Participating Agencies are required to provide a printout from HMIS of the Universal and Program Specific Data Elements.
- Participating Agencies are not required to print out any additional information, although it is optional and allowed.

Best Practices:

- Case management notes are typically not shared with the client. However, consider providing the client related information such as their goals, outcomes, referrals, and services provided.
- If utilizing paper forms, with data entry occurring later, consider making a photocopy of the paper forms for the client if they request a copy.
- If entering data directly, without utilizing paper forms, consider automatically printing a copy of the information for the client.

6.4 Client Grievance Process

Policy:

Clients have the right to file a Grievance Form regarding potential violation of their privacy rights as it pertains to HMIS participation.

Procedures:

- A client must request the Client HMIS Grievance Form (Appendix G) from the Participating Agency.
- The client may choose to submit the completed form to the Participating Agency, OR the client may submit the form directly to the HMIS System Administrator .
- If the Participating Agency receives a completed Grievance Form, they must submit it to the HMIS System Administrator by the end of the next business day.
- The HMIS System Administrator will review the grievance, research the nature of the complaint, and will respond to the grievant within 30 days.

Policy:

No punishment will be taken by the HMIS Committee against a client if a client files a grievance.

Procedure:

- The Participating Agency named in the grievance, the HMIS System Administrator , and other Participating Agencies will not refuse or reduce services to the client because of a grievance.
- If a client reports retaliation because of filing a grievance, the HMIS Committee will conduct an investigation.

6.5 Electronic Sharing of Client Data

Policy:

HMIS has the ability to allow client information sharing between Participating Agencies. Client data may be shared if: 1) it is explicitly authorized by the client on the Release of Information form and 2) an Inter-Agency Data Sharing Agreement has been executed by the Participating Agency.

Description:

While coordinating services, it is important to keep the Client's identity confidential unless the Client expressly permits their information to be shared by signing a Client Consent Form-Release of Information (ROI) and the Participating Agency has signed an Inter-Agency Data Sharing Agreement (Appendix E).

Procedures:

- End Users will keep client data confidential at all times and will obtain client permission to disclose Personally Identifiable Information only when necessary or otherwise required by law or court order.
 - Electronic data sharing between Participating Agencies will be enabled with client consent.
-

7. SECURITY STANDARDS

Through a set of administrative, physical and technical safeguards, the security standards are to: (1) ensure the confidentiality, integrity, and availability of all HMIS information; (2) protect against any reasonably anticipated threats or hazards to security; and (3) ensure compliance by Participating Agency End Users.

7.1 Security Management

Policy:

The HMIS System Administrator will update and maintain the Security Plan as directed

7.1.1 Security Plan

The Security Plan is attached to these guidelines as Appendix L.

7.2 Workstation Security Procedures

Most security breaches are due to human error rather than systematic issues. To keep the application and data secure, Participating Agency End Users must implement security measures.

Policy:

Participating Agency End Users' computer screens should be placed where those not authorized to view confidential data are unable to see the contents of the screen.

Description:

The placement of the monitor can play a role in establishing security at the Participating Agency. Participating Agency End Users will position the monitor in a way that it is difficult for others to see the screen.

Best Practice:

Participating Agencies must determine the best location for computer monitors to prohibit unauthorized viewing of the computer screen. Another option is to utilize a privacy filter for the monitor.

Policy:

Do not write down usernames and/or passwords and store them in an unsecured manner.

Description:

Do not post HMIS username or password information under keyboards, on monitors, or within public view. This type of behavior can lead to large security breaches. Passwords and usernames that are written down must be secured in a locked drawer.

Policy:

Do not ever share login information with anybody (including Participating Agency HMIS Lead or HMIS System Administrator).

Description:

If someone is having trouble accessing HMIS, direct them to contact the Participating Agency HMIS Lead or call or send an e-mail to the HMIS System Administrator. Sharing usernames and passwords or logging on for someone else is a serious security violation of the HMIS End User Agreement (Appendix H). Participating Agency End Users are responsible for all actions taken in the system utilizing their logons. With the auditing and logging mechanisms within HMIS, any changes made, or actions taken will be tracked back to that login.

Policy:

When the Participating Agency End User is away from their computer, the Participating Agency End User must log out of HMIS or lockdown the workstation.

Description:

Stepping away from the computer while logged into HMIS can lead to a serious security breach. Although there are timeouts in place to catch inactivity built into the software, it does not take effect immediately. Therefore, anytime the Participating Agency End User leaves their computer, one of two actions must be completed. The Participating Agency End User can lock down the workstation or log out of HMIS.

7.3 HMIS Software Application – Level Security

Within the HMIS software itself, there are additional layers of security. This makes the system harder to access without appropriate permissions. These security features include:

- There is an SSL encryption of the connection between a Participating Agency End User's computer and the HMIS application. Advanced Encryption Standard, 256-bit, is the method in which the data is encrypted.
 - Firewalls are in place on all servers hosted by WellSky. WellSky utilizes an industry standard Intrusion Detection System to pinpoint unauthorized attempts at accessing its network and to shield the customer's data in the event of such an attempt.
 - Participating Agency End Users are organized into visibility groups. The groups are given specific permissions on what they can access.
 - A Participating Agency End User's connection to the HMIS application will automatically close down after a period of inactivity.
 - There are logging and auditing systems in the background recording each Participating Agency End User's activities in adding, viewing, and editing information.
-

7.4 Security Review

Policy:

The HMIS System Administrator must complete an annual security review to ensure the implementation of the security requirements by Participating Agencies and the HMIS System Administrator, itself. This security review will include the completion of a security checklist ensuring that each of the security standards is implemented in accordance with the HMIS security plan.

Description:

Each Participating Agency is given, at time of training, suggestions for providing a secure environment for their clients and Participating Agency End Users who utilize HMIS. Once a year, a security review is conducted at each Participating Agency's location. The following areas of security will be examined and documented:

- Physical and Environmental Security
- PC location out of public area
- Printer location
- PC access
- Personnel Security
- Passwords
- Signed Agreements
- Number of authorized users

Procedures:

- The security review may be carried out by 2 different methods: (1) HMIS Administrator; or (2) HMIS/CEP Committee designee.
- The HMIS System Administrator or a designee will notify the Participating Agency Security Officer of an upcoming review.
- A report with the results of the security review will be submitted to the Participating Agency Security Officer and the HMIS/CEP Committee. A copy will be filed at the HMIS System Administrator's office.
- Any deficiencies in practices or security must be resolved immediately. A follow-up review will be conducted to ensure that the changes have taken effect.

Policy:

Participating Agencies are required to immediately resolve any issues discovered during a security review.

Description:

Within 30 days of the Participating Agency security review report, the Participating Agency must provide a written response. The response will be reviewed by the HMIS Committee for clearance and compliance with these Policies and Procedures.

8. HMIS IMPLEMENTATION

8.1 HMIS Software Solution

The NorCal CA 516 has selected “Community Services (formerly ServicePoint)”, a web based HMIS software owned by WellSky to be the HMIS software of record. It empowers human service providers, agencies, coalitions, and communities to manage real-time client and services data. The City of Redding as the Administrative Entity for the NorCal CoC (Administrative Entity) will contract directly with WellSky for this software and supports end-users with a help desk, ongoing training, and project customization including development of project-specific assessments and settings.

8.2 Technology Requirements

Policy:

All computers authorized to access Community Services must meet the minimum requirements as established in this manual.

Procedures:

All computers that will access Community Services (ServicePoint) on behalf of the Participating Agency must meet these minimum requirements; this includes Participating Agency's on-site desktops and laptops. **Accessing Community Services (ServicePoint) from home is never allowed due to security breaches.** It is difficult to ensure that a computer in the home meets the technical standards and that Participating Agency End Users are abiding by the same privacy, confidentiality, and security procedures as they would in the office. Unauthorized individuals (spouses, children, and relatives) could gain access to Community Services (ServicePoint) in a home environment more easily than in an office environment.

Participating Agencies must ensure that their computers meet the following standards:

Supported Browser Brands

Apple Safari
Google Chrome
Microsoft Edge
Microsoft Internet Explorer 11

Java

Required	Recommended
Any version of Java	Recent version of Java

Mobile Devices

Apple iPad with latest version of IOS

Operating Systems

All operating systems used by Participating Agencies must receive support from Microsoft or Apple with regular updates to current operating system. For Microsoft life cycle policy, please find your operating system here: <https://support.microsoft.com/en-us/lifecycle/selectindex>.

Best Practices:

Participating Agencies should consider these recommendations in preparation for fully utilizing all the capabilities within Community Services (ServicePoint) as well as incorporating standard industry practices:

- Operating system version: Each computer should be on a currently supported version of an operating system (e.g. Windows XP, Windows Vista, Windows 7, Windows 8, or Mac O/S 10.3 or higher).
- Operating system updates: Each computer accessing Community Services (ServicePoint) should be current in applying all of the available critical security patches. Patches should be installed within 24 hours of notification of availability.
- Current anti-virus software and firewall should be present and active.
- Anti-Spyware software: For a computer or network, anti-spyware software should be present, active, and with current definitions.
- Secure internet connection: Ideally each computer should have access to at least a DSL/Broadband high-speed line instead of dial-up connection. This will result in a much-improved experience over connecting with dial-up speeds.
- Standard office software: To use downloaded data from Community Services software that can interpret comma-delimited files, such as spreadsheet, word processing, or database software (such as Microsoft's Excel, Word, and Access) should be present. There are a number of options. It is not a requirement that this software is installed since it is not required to enter HMIS data.

8.3 Inter-Agency Data Sharing Agreement

Policy:

To systematically share data, the Participating Agencies will jointly establish a data sharing network formalized by the execution of an HMIS Inter-Agency Data Sharing Agreement. (Appendix E).

Description:

The Inter-Agency Data Sharing Agreement is a contract between the Participating Agencies who agree to share information in HMIS. The agreement outlines specific requirements on confidentiality, data entry, responsibilities, security, reporting, and other items deemed necessary for proper HMIS operation and compliance.

Procedures:

- An authorized representative of the Participating Agency will sign the Inter-Agency Data Sharing Agreement. Each will maintain a copy for their files.
- The original will be filed at the Administrative Entity.

8.4 End User Agreements

Policy:

An End User Agreement (Appendix H) must be signed and kept for all Participating Agency's personnel or volunteers that will collect, use or view data on behalf of the Participating Agency.

Description:

The HMIS End User Agreement is an agreement between the HMIS System Administrator and a Participating Agency's employees, contractors, or volunteers who are authorized to collect and/or enter data.

Procedures:

- Before a Participating Agency End User begins collecting data, the Participating Agency End User and their program manager must sign an HMIS End User Agreement.
- The HMIS System Administrator must retain the signed HMIS End User Agreement until seven years after user access is terminated.
- The Participating Agency must ensure that each Participating Agency End User has been trained by the HMIS System Administrator.
- All end user accounts are subject to a 90-day activity review. If an end user does not login to HMIS within a 90-day period, their access will be deactivated. This access can be reactivated by the Agency's HMIS Lead emailing the HMIS Administrator: HMIS@NorCalUnitedWay.org. The request must include the user's information and the reason as to why the end user had not logged into ServicePoint within the prior 90 days and why the user still needs access. All end users that have been deactivated for 6 months or more must attend additional training.

8.4.1 Removing Authorized Personnel**Policy:**

The HMIS System Administrator must be notified as soon as possible, but no later than 3 business days when a Participating Agency End User is no longer authorized to access HMIS.

Procedures:

- Within 3 business days of revoking a Participating Agency's End User's authorization, the Participating Agency will contact the System Administrator via email HMIS@NorCalUnitedWay.org.
- The Participating Agency will email the System Administrator at the above email address or fax it to 530-225-5178.
- Upon receipt of the User Account Request Form, the HMIS System Administrator will immediately deactivate and/or delete the Participating Agency End User's account.

8.5 HMIS Licensing**Policy:**

To participate in HMIS, the Participating Agency must obtain a username for each Participating Agency End User.

Description:

To participate in HMIS, each Participating Agency must have a minimum of one Community Services (ServicePoint) license allowing for one Participating Agency End User.

Procedure:

- When new agencies are requesting participation, a site visit may be scheduled, and all policy and security requirements will be evaluated by the HMIS System Administrator .

8.6 Designate Participating Agency HMIS Lead

Policy:

All Participating Agencies must designate a Participating Agency HMIS Lead.

Description:

The Participating Agency must designate an individual to act as their Participating Agency HMIS Lead.

The Participating Agency HMIS Lead role possesses different responsibilities than a typical Participating Agency End User. The Participating Agency HMIS Lead will:

- Act as the first tier of support for Participating Agency End Users.
- Act as the main point of contact for HMIS System Administrator for HMIS related issues.
- Ensure compliance with these Policies and Procedures.
- Post the Mandatory Collection Notice.
- Assist Participating Agency End Users with technical assistance and monitoring.
- **Be a member of and attend HMIS/CE Committee meetings.**
- Request Participating Agency End User additions and deletions as appropriate.
- Request training and/or technical assistance.
- Run the required Reports for each of the Participating Agency's programs based on the reporting schedule and respond to the HMIS System Administrator 's request for data clean-up.

Procedures:

The Participating Agency's HMIS Lead is designated as an oversight person and has the overall responsibility for meeting the requirements of these Policies and Procedures.

8.7 Participating Agency Profile in HMIS

Policy:

Participating Agencies are not able to enter Client data until their profile is set up in Community Services (ServicePoint)

Description:

Within HMIS, each Participating Agency will have an organizational profile that contains the programs and services the Participating Agency offers. The HMIS Administrator will work with each Participating Agency individually to design their profiles.

Procedures:

- The Participating Agency HMIS Lead will work with the HMIS System Administrator to complete the agency profile set up.
- The HMIS System Administrator will work with the Participating Agency HMIS Lead to ensure that the profiles are organized in a way that is useful for the Participating Agency, consistent with standard practices, and meets reporting needs.

8.8 Designating Participating Agency End Users

Policy:

Any individual working on behalf of the Participating Agency (ex: employee, contractor, and/or volunteer), who will collect information for HMIS purposes must be designated as a Participating Agency End User; and therefore, is subject to these Policies and Procedures.

Description:

Anyone who collects HMIS data (electronic or paper) or creates reports from Community Services (ServicePoint) must be designated as a Participating Agency End User. Due to client privacy, confidentiality, and security procedures, all Participating Agency End Users must follow the standards and procedures set forth for security and confidentiality. Participating Agency End Users who have not had the proper training will not be equipped to respond to Clients' questions on consent, revocation, intake forms, and other aspects. An individual, who is designated as a Participating Agency End User, but that does not work within Community Services (ServicePoint), is still required to take the Policies and Procedures training class. Individuals who do work within Community Services (ServicePoint) will take this class, as well as specific training on Community Services (ServicePoint).

Procedures:

- After an individual is identified as a Participating Agency End User, the Participating Agency HMIS Lead must sign the End User Agreement Form for submission to the HMIS System Administrator.
 - The individual is required to complete the appropriate user training as determined by the HMIS System Administrator and/or the project supervisor.
-

9. DATA COLLECTION & REPORTING

9.1 On Whom to Collect Data

Policy:

Participating Agencies are required to attempt data collection with individuals who are experiencing homelessness or are at risk of experiencing homelessness and who are receiving services

Procedures:

- For HMIS purposes, HUD's minimum standards require that individuals who are experiencing homelessness or are at risk of experiencing homelessness and receive services from a Participating Agency must be approached for data collection. Therefore, during the intake process it is important to identify these persons.
- Once these persons are identified, they must go through the Informed Consent Process, which is an oral explanation of HMIS and its benefits, as well as the Client's rights in regard to HMIS.
- Information must be collected separately for each family member, rather than collecting data for the family as a whole.

Best Practices:

- Participating Agencies should also collect HMIS data for individuals or families at risk of homelessness but who are receiving services from the Participating Agency. One of the greatest benefits of HMIS to a Participating Agency is the ability to create reports describing its clients' characteristics, outcomes of the services they receive, and general agency operating information. Entering HMIS data only for persons experiencing homelessness will give the Participating Agency a partial picture. By including both persons already experiencing homelessness and persons at risk of homelessness, Participating Agencies will be able to generate reports that wholly describe their operations.
- Participating Agencies should collect data on individuals or families experiencing homelessness that make contact with the Participating Agency. Enrolling those individuals in Coordinated Entry allows HMIS Participating Agencies the ability to count the persons that attempt to enroll in programs/services, even though they may not actually end up receiving those services. The Participating Agency will be able to create reports about the characteristics of these individuals and use this information for a number of reasons. The Participating Agency could use this data to determine if they are being improperly referred or to quantify the additional need for funding.

9.2 Using Paper-based Data Collection Forms

Policy:

Participating Agencies may choose to collect client data on paper for later data entry or for assistance in data entry. Participating Agencies must use the HMIS Intake Form (Appendix I) provided by the System Administrator .

Description:

Each Participating Agency will incorporate HMIS into its own operating processes. Some Participating Agencies will prefer to interview clients and simultaneously enter their information directly into the computer. Other Participating Agencies will find it easier to collect information on paper first, and then have someone enter the data later into the HMIS. HMIS paper-based forms that enable collection of the Universal, and Program Specific Data Standards are available. Participating Agencies should use:

- Adult Intake form (Appendix I)
- Minor Intake Form (Appendix J)
- Interim/Exit Form (Appendix K)
- Client Consent Form - Release of Information (ROI) (Appendix A)

During the HMIS training, Participating Agency End Users will learn how to use these forms to fulfill their data collection obligations.

Procedures:

- Participating Agencies may utilize paper-based forms for initial data collection.
- Participating Agency End Users will have 5 business days or 7 calendar days from the point of the event (intake/enrollment, service delivery, or exit) to enter the data.
- Standard forms provided by the HMIS System Administrator to capture Universal and Program Specific data shall be used by Participating Agencies using paper-based forms for data collection.

9.3 Client Intake: Completing Required Fields in HMIS**Policy:**

During client intake, Participating Agency End Users must complete the Universal and Program Specific fields as required for all clients.

Description:

All Participating Agencies are required to complete the Universal fields regardless of funding sources. Participating Agencies that receive homeless assistance grant funds from HUD and the CoC are required to complete the Program Specific fields.

Procedures:

- To complete the Universal fields for intake, Participating Agency End Users will follow the workflow that is set up for their program.
- To complete the Program Specific required fields, Participating Agency End Users will follow the workflow that is set up for their program.

Best Practice:

Participating Agency End Users should be aware of their Participating Agency's data requirements and internal standards. Participating Agencies may decide to collect additional pieces of information beyond the Universal and Program Specific fields. Such additional data needed for the Participating Agency's own operations and/or funding

sources can be entered into HMIS. The Participating Agency will contact the HMIS Administrator to discuss the additional data requirements that need to be collected.

9.5 Client Discharge: Exiting Clients from Programs

Policy:

During discharge or program exit, Participating Agency End Users must complete the Universal and Program Specific required fields for all clients within 5 business days or 7 calendar days.

Description:

During client discharge from a program, there are additional data collection requirements.

Procedures:

- Participating Agency End Users must complete the Universal and Program Specific required fields for discharge.
 - To complete the Program Specific required fields, End Users must go to the *Client Program Close, Program Exit, Special Needs at Exit, Income at Exit, Income at Exit Summary and Outcomes* screens and respond to the fields marked required.
 - If a Participating Agency collects data on paper-based data forms, the Exit form (Appendix K) shall be used.
-

10. TRAINING & TECHNICAL ASSISTANCE

10.1 End User Training

Policy:

Participating Agency End Users are required to complete new user training before access to HMIS is given.

Description:

The following training, at a minimum, will be provided quarterly:

Training		
Course Description	Course Detail	Required
HMIS Part 1	Policies and Procedures, review of HMIS Data and Technical Standards, Privacy and Mandatory Collection Notices and Consents, navigating HMIS	All new Participating Agency end-users
HMIS Part 2	Policies and Procedures, Setting Up Households, Household Data Sharing, Interim/Annual Updates, Exits and Referrals	All new Participating Agency end users
HMIS Refresher	Review of navigating HMIS, review of HMIS Data and Technical Standards, Review of Privacy, Security and Policies and Procedures	All existing Participating Agency end-users, annually
Reports	Running and understanding management reports; Data clean-up	All new Participating Agency end-users, as needed basis

Procedures:

There are several prerequisites for attending the Participating Agency End User training:

- The Participating Agency must have signed and returned the MOU between UWNC and the Participating Agency and have paid for their annual license(s).
- All Participating Agency HMIS Leads can request End User training by emailing to the HMIS System Administrator.
Email: HMIS@NorCalUnitedWay.org
- Participating Agency HMIS Leads shall contact the HMIS System Administrator for information on when the next training is being offered. Training spots are allocated on a first-come first-serve basis.
- Upon completion of training, Participating Agency End Users will be given a login and password to provide access to Community Services (ServicePoint). At this point, the End User will be able to utilize Community Services (ServicePoint).

10.2 Training Refresher

Policy:

All Participating Agencies may request a training refresher as needed.

Description:

HMIS will evolve over time to include new HUD requirements as well as functions that Participating Agencies and the community request.

Procedures:

The Participating Agency HMIS Lead shall contact the HMIS System Administrator to request any additional training necessary to maintain compliance with these Policies and Procedures.

10.3 Contacting the System Administrator

Policy:

All requests for technical assistance and training shall be requested by the Participating Agency HMIS Lead

Procedures:

HMIS System Administrator will be the best resource for finding out specific information regarding technical issues and reporting. Contact the HMIS System Administrator by email at HMIS@NorCalUnitedWay.org.

Appendix A: HMIS Client Consent Form

Homeless Management Information System (HMIS)
Authorization to Use or Disclose Confidential Information

I hereby authorize use or disclosure of the named individuals' confidential information (CI) collected in the Vulnerability Index, as described below. I understand this authorization may include the disclosure or exchange of information in written, verbal, electronic and/or other forms. The named individuals' CI will not be made public and will only be used with strict confidentiality.

Client:

Last Name: _____ First Name: _____
Address: _____
City: _____ State: _____ Zip: _____
Telephone Number: _____
Date of Birth: _____

I understand that _____ (Service Provider) collected information about me and/or my dependents listed below to enter it into a database system called Homeless Management Information System (HMIS). This database helps the Continuum of Care (CoC) members and HUD to better understand homelessness, to improve service delivery to the homeless, and to evaluate the effectiveness of services provided to the homeless in the CoC. Participation in data collection and release, although optional, is a critical component of our community's ability to provide the most effective services and housing. The information that is collected in the HMIS database is protected by limiting access to the database and by limiting with whom the information may be shared, in compliance with the standards set forth by federal, state, and local regulations governing confidentiality of client records. Every person and agency that is authorized to read or enter information into the database has signed an agreement to maintain the security and confidentiality of the information.

The CI gathered and prepared will be included in a HMIS database of participating agencies who have entered into a Data Sharing Agreement and shall be used to:

- a. Produce a client profile at intake that will be shared by collaborating agencies
- b. Produce anonymous, aggregate-level reports regarding use of services
- c. Track individual program-level outcomes
- d. Identify unfilled service needs and plan for the provision of new services
- e. Allocate resources among agencies engaged in the provision of new services
- f. Disclose if required by court order or as required by law
- g. Assess needs for housing, utility assistance, food, counseling and/or other services.

The information may include, but is not limited to the following CI:

- Full Name
 - Date of Birth
 - Social Security Number
 - Gender
 - Ethnicity & Race
 - Veteran Status
 - Program entry date
 - Program exit date
 - CIN/insurance
 - Residence prior to project entry
 - HIV/AIDS status
 - Homeless history
 - Zip Codes of last permanent address
 - Family composition
 - Employment status
 - Housing information
 - Income and benefits information
 - Domestic Violence
 - Mental Health
 - Disabling condition
 - Alcohol & drug
 - Legal history
 - Photo (if applicable)
- The release of my information listed above does not guarantee that I will receive assistance, and my refusal to authorize the use of my information does not disqualify me from receiving assistance.
 - I may revoke this authorization at any time by signing a “Revocation of Consent to Release Information form”.
 - I understand the revocation will not apply to information already released based on this authorization, and all information about me already in the database will remain but will become invisible to all of the participating agencies.
 - My records are protected by federal, state, and local regulations governing confidentiality of client records and cannot be disclosed without my written consent unless otherwise provided for in the regulations, law, or court order.
 - Auditors or funders who have legal rights to review the work of this agency, including the U.S. Department of Housing & Urban Development and Department of Healthcare Services may see my information.
 - People using HMIS information to write reports may see my information. Researchers must sign an agreement to protect and deidentify CI before seeing HMIS data.
 - I understand I may inspect or obtain a copy of the CI to be used or disclosed. I have the right to receive a copy of this authorization.
 - This authorization is valid for three (3) years from the date of my signature below or the 18th birthday of the minor dependent, whichever occurs first.

Participating agencies: Agencies within the NorCal Continuum of Care HMIS are authorized to use, disclose, and obtain information from the HMIS database are listed below. These agencies may update periodically and can have retroactive effectiveness:

Del Norte:

County of Del Norte
Del Norte Mission Possible
Crescent City

Lassen:

Lassen County HSS
Susanville Indian Rancheria

Modoc County:

TEACH
Modoc County

Plumas:

Plumas Crisis Intervention Resource Center
Plumas County Behavioral Health

Sierra County:

Sierra County

Shasta:

Faithworks
No Boundaries
Good News Rescue Mission
Nation's Finest
Pathways to Housing
Ready for Life
Hill Country Community Clinic
Shasta Community Health Center
Access Homes
Shasta County HHSA
Shasta County Housing Authority
City of Redding
Lutheran Social Services
North Valley Catholic Social Services
Northern California Youth and Family Programs
Shasta County Office of Education
United Way

Siskiyou County:

Siskiyou County HHSA
Karuk Tribe
Youth Empowerment Siskiyou

Partnership Health Plan of California

Please initial one of the following levels of consent:

_____ I give authorization for confidential information **to be entered into HMIS and shared between participating agencies.**

OR

_____ I do not consent to the inclusion of confidential information in HMIS.

I, _____(name of parent or legal guardian), am the parent or legal guardian of child(ren) listed below) and have legal authority to execute this Release.

My signature on this document is intended to bind myself, my child or any child whom I have legal custody and control of and for whom I have the authority to execute this release. The undersigned expressly agrees that this Release is intended to be as broad and inclusive as permitted by California law.

List all Dependent children under 18 in household, if any (first and last names):

1.	2.
3.	4.
5.	6.
7.	8.

Printed name

Date

Signature

Relationship to Client

Appendix B: Privacy Policy

**NorCal CA 516 Continuum of Care
Homeless Management Information System (HMIS)
Notice of Privacy Practices**

**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:

United Way of Northern California
3300 Churn Creek Road, Redding CA, 96002
(530) 241-7521

Your information is personal, and the NorCal CA 516 Continuum of Care 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 any member of staff, or go to the United Way of Northern California website at: <https://www.norcalunitedway.org/hmis>.

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.

Participating agencies 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.

Participating agencies may use and disclose your information to other participating HMIS agencies.

We also 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 Collaboration: We also may use and disclose your information about you so that you do not have 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.

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 level 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 the use or disclosure of information for research purposes, any such research project must be

approved through an approval process. Aggregate information about you may be disclosed to people conducting a research project to help them identify data for clients with specific needs.

As Required By Law: We will use and disclose information when required 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 an oversight agency, such as the Department of Housing and Urban Development (HUD) or the State of California, for activities authorized by law. These oversight activities are necessary for the government to monitor government service programs, and compliance with civil rights laws.

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. The request will be reviewed and responded to within three (3) business days. We reserve the right to deny your right to inspect and obtain copies of your information. If your request is denied, you may appeal this decision and request another services professional at United Way of Northern California, who was not involved in your provision of services, review the denial.

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. Your request will become part of your record.

Right to Request Restrictions:

You have the right to request that we follow additional, special restrictions when disclosing your information. 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 service 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 member of staff.

You have the right to file a complaint if you believe that 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 NorCal CA 516 Continuum of Care System Administrator.

To file a complaint with the Lead Agency, contact:
United Way of Northern California
3300 Churn Creek Road, Redding CA 96002 Email:

HMIS@NorCalUnitedWay.org

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: <https://www.norcalunitedway.org/hmis> or by contacting any staff person involved in your services.

If you have any questions about our Notice of Privacy Practices, please contact: United Way of Northern California
3300 Churn Creek Road, Redding CA 96002 Email:

HMIS@NorCalUnitedWay.org

I acknowledge receipt of the HMIS Notice of Privacy Practices.

_____	_____	_____
Client Signature	Client Printed Name	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	Date

Appendix C: Mandatory Collection Notice

HOMELESS MANAGEMENT INFORMATION SYSTEM MANDATORY COLLECTION NOTICE

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

Appendix D: HMIS Request for Policy Addition, Deletion, or Change

NorCal CA 516 Continuum of Care
HMIS Request for Policy Addition, Deletion, Change

Organization: _____

Name: _____

Date: _____

I request that the following change(s) be made to the HMIS Policies & Procedures Manual:

Change the following existing policy:

Delete the following existing policy:

Add the following:

Provide in clear and concise language the policy to be considered by the HMIS Committee to be inserted / deleted in or from the current Policies and Procedures manual. Please be clear and specific.

Policy:

Provide a brief description of the policy or process. Please be clear and specific.

Description:

Provide in detail the procedure for the policy identified above. Please be clear and specific.

Procedures:

Appendix E: Inter-Agency Data Sharing Agreement

NorCal CA 516 Inter-Agency HMIS Data Sharing Agreement

By signing this Inter-Agency Data Sharing Agreement, _____ shall be designated a "Participating Agency" in the NorCal CA-516 Homeless Management Information System (HMIS) and/or Coordinated Entry Process (CEP). This Participating Agency agrees to share the demographic and programmatic data (when authorized to do so by the client) using the NorCal CA 516 HMIS or during CEP case conferencing. The Participating Agency's client data shall be shared with all participating agencies that also have a signed Inter-Agency Data Sharing Agreement on file with the HMIS System Administrator (United Way of Northern California). Each individual end user that directly accesses and enters data into HMIS must complete and comply with the HMIS User Agreement.

Authorized Uses and Disclosures of HMIS Data¹:

- To provide or coordinate housing and/or services for families and individuals experiencing homelessness or facing a housing crisis across the NorCal Continuum of Care service area which includes the counties of Del Norte, Lassen, Modoc, Plumas, Shasta, Sierra, and Siskiyou.
- For functions related to payment or reimbursement for services.
- To carry out administrative functions, including but not limited to legal, audit, personnel oversight and management functions.
- For creating de-identified reports from PII.
- To avert a serious threat to health or safety.
- Uses and discloses for academic research purposes.
- Disclosures for law enforcement purposes.

Participating Agency Requirements:

Each Participating Agency agrees that it shall:

- With respect to any and all information, only obtain, use, and disclose information in accordance with HMIS Policies & Procedures. The Participating Agency will produce a client profile at intake that will be shared by collaborating agencies.
- Produce anonymous, aggregate-level reports regarding use of services to identify unfilled service needs and plan for the provision of new services, allocate resources among agencies engaged in the provision of new services and track individual program-level outcomes.
- Not access identifying information for any individual who is (a) not a client of the Participating Agency or (b) who has not consented in writing to share, disclose, or release of information. The Participating Agency may access its clients' identifying information on an as needed basis and request in writing access to statistical, non-identifying information on clients served by other Participating Agencies.
- Not report on a client's whereabouts to outside entities that are not a part of this signed Inter-Agency Data Sharing Agreement (e.g., law enforcement, missing person inquiries, and governmental agencies), unless required by law, court order or other requirements, or if life threatening or emergency circumstances warrant.
- Report only non-identifying information from HMIS in response to requests unless otherwise required by law.

¹Federal Register/Vol.69, No. 146, Friday, July 30, 2004

Client Protection:

- Basic client profile data, which includes client demographics (name, birth date, social security number, gender, ethnicity, veteran status, language(s) spoken, photo, other identifying information, etc.) will be shared with the NorCal CoC Participating Agencies participating in HMIS provided that the client to whom the data pertains has in place a current, valid written consent, for the obtaining, disclosure, sharing, and release of that information and that the consent has not been withdrawn or revoked.
- The applicable Client Authorization form (ROI) must be signed by the client in order for the Personally Identifiable Information (PII) to be shared in HMIS or during CEP case conferencing.
- In the event a client doesn't want to share their information with other agencies, it's the responsibility of the Participating Agency end-user to make client's program enrollment, services, file, etc., private in HMIS and to ensure if the information is provided during CEP case conferencing, it is done so in a non-identifying manner. .
- Client's project level information (services, VI-SPDAT assessments, project placement history, forms, documents, and contact information) will only be shared among the agencies that have signed this agreement. At the time of informed consent, and at any point after, the client has the right to revoke consent. Any revocation of consent is effective from the date of revocation going forward and does not apply to data that is already shared in HMIS or for the purposes of CEP case conferencing.
- HMIS Participating Agency 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 (see the Client Informed Consent & Release of Information Authorization and the Notice of Privacy Practices in HMIS Policies and Procedures both within HMIS and during CEP case conferencing.
- Clients may NOT be denied services based on their choice to withhold their consent to share their information.

Agreed to and signed by the following agency representative:

Printed Name

Agency Name

Signature

Date

Appendix F: Revocation Form

NorCal CA 516Homeless Management Information System (HMIS)

Client Revocation Form

Agency Information ("This agency") _____

Name: _____

Address: _____

City, State, Zip: _____

I hereby revoke permission for this agency to share my demographic, household and service information with other agencies that use NorCal CA 516Homeless Management Information System (HMIS).

I understand that the information will remain in HMIS, and will no longer be available to other partner agencies; however, information previously shared or disclosed by this agency as a result of my prior consent cannot be retracted, nor may this agency withhold information required to be shared or disclosed by law.

Name of Client

Signature of Client

Date

Name of Agency Representative

Signature of Agency Representative

Date

Appendix G: Client HMIS Grievance Form

NorCal CA 516 HMIS

If you think your privacy rights for the information entered into HMIS have been violated, use this form to report the problem.

It is against the law for any agency to retaliate against you or deny services for the act of filing a grievance.

Name of Individual Filing the Grievance: _____		
Grievance Information		
Date of Occurrence: _____	Have you discussed this issue with the HMIS Agency? Yes No Date of discussion: _____	Agency Name:
Issue of Grievance: List specific problem(s)/issue(s). 		
For clarification of the issues of your grievance, please provide statements regarding the condition which is the subject of this grievance. (Describe what happened, when, and where. Attach any supporting documentation.) 		
Relief Request: Indicate the action(s) that would resolve your grievance. 		

My signature indicates that the information contained on this form and attachments (if any) to this form is true and factual to the best of my knowledge.

Signature

Date

Appendix H: HMIS End User Agreement

HMIS USER AGREEMENT

Agency: _____ Name of End User: _____

The NorCal CoC recognizes the importance of client needs in the design and management of HMIS. These needs include maintaining client confidentiality and treating the personal data of clients with respect and care.

As the guardians entrusted with this personal data, Participating Agency End Users have a moral and a legal obligation to ensure that the data they enter into HMIS is being collected, accessed and used appropriately. Proper user training; adherence to the NorCal HMIS Policies and Procedures Manual; and a clear understanding of the privacy, security, and confidentiality policies are vital to achieving these goals.

Your User ID and password give you access to HMIS. Initial each item below to indicate your understanding and acceptance of the proper use of your User ID and password and your intention to comply with all elements of the Homeless Management Information System Data and Technical Standards Notice published by the U.S. Department of Housing and Urban Development. Unauthorized use or disclosure of HMIS information is a serious matter and any End User found to be in breach of this agreement will be subject to the following penalties or sanctions, including: the loss or limitation of use of Service Point; adverse employment actions including dismissal; and civil and/or criminal prosecution.

Please initial that you understand and agree to comply with all the statements listed below.

_____ My ServicePoint User ID and password are for my use only and must not be shared with anyone. (Licensed User Only)

_____ I will take all reasonable means to keep my User ID and password physically secure. (Licensed User Only)

_____ If I am logged into ServicePoint and must leave the work area where the computer is located, I must log-off of Service Point before leaving. (Licensed User Only)

_____ Any computer that has Service Point "open and running" shall never be left unattended. Any computer that is used to access Service Point must be equipped with locking (password protected) screen savers.

_____ If I notice or suspect a security breach, I must notify the HMIS System Administrator.

_____ I understand that the only individuals who can view HMIS information are authorized users and the clients to whom the information pertains.

_____ I understand that in the event a client doesn't want to share their information with other agencies, it's my responsibility to make the client's program enrollment, services, file, etc., private in HMIS and to ensure if the information is provided during CEP case conferencing; it is done so in a non-identifying manner.

_____ I understand that I will maintain HMIS data in such a way as to protect against revealing the identity of clients to unauthorized agencies, individuals, or entities (see the Client informed Consent and Release of Information Authorization and the Notice of Privacy Practices in HMIS Policies and Procedures) both within HMIS and during CPE case conferencing.

_____ I understand that I may only view, obtain, disclose, or use the database information that is necessary in performing my job.

_____ I understand that these rules apply to all users of HMIS, whatever their work role or position.

_____ I understand that hard copies of HMIS information must be kept in a secure file.

_____ I understand that once hard copies of HMIS information are no longer needed, they must be properly destroyed to maintain confidentiality.

I affirm the following:

1. I have received the following HMIS trainings:

a) ServicePoint use (Licensed User Only)

b) Privacy

c) Data collection

d) Security policy

2. I have read and will abide by all policies and procedures in the HMIS Policies and Procedures Manual and have adequate training and knowledge to enter data and/or run reports in ServicePoint.

3. I will maintain the confidentiality of client data in ServicePoint as outlined above and in the HMIS Policies and Procedures Manual.

4. I will only search, view, enter or share data in HMIS when a Client Consent Form is on file.

End User Signature

Date

End User Printed Name

Phone Number

Email Address

To be filled out by Agency Directory/Supervisor

Designated Agency HMIS Program Lead ☐Yes ☐No User

will be generating reports ☐Yes ☐No **Non-**

Licensed Users

Volunteer ☐Yes ☐No

Data Collection Only ☐Yes ☐No

Please indicate the programs the end user has been authorized to access.

1. _____ 2. _____ 3. _____

4. _____ 5. _____ 6. _____

Agency Director/ Supervisor

Date

Appendix I: Adult Intake Form

1. Intake Summary									
Agency Case No:					Service Point Client No:				
Intake Date	Mont	Day	Year	Intake Staff Name					
Case Manager				Staff Direct Phone Line					
Agency Name				Notice of Privacy Practices Acknowledgement signed ☐ Yes ☐ No					
Program Name				Release of Information (ROI) Signed ☐ Yes ☐ No					
2. Household Information									
Household Type	☐ Couple (parent & friend) & child(ren)			☐ Foster Parent(s)with child(ren)			☐ Other		
	☐ Couple with no child(ren)			☐ Grandparent(s)with child(ren)			☐ Single Adult		
	☐ Extended family unit			☐ Male Single Parent			☐ Two Parents with child(ren)		
	☐ Female Single Parent			☐ Non-custodial Caregiver(s)w/child(ren)					
3. Client Information									
First			Middle		Last			Suffix	
Alias			Email Address						
Address					Telephone				
SSN	- -			U.S. Military Veteran <i>(adults only)</i>		☐ Yes			
SSN Data Quality	☐ Full Reported ☐ Partial/Approx. Reported ☐ Client doesn't know ☐ Client refused					☐ No ☐ Client doesn't know ☐ Client refused			
Date of Birth	Month	Day	Year	Gender		☐ Male ☐ Female ☐ A gender other than singularly female or male (e.g., non-binary, genderfluid, agender, culturally specific gender) ☐ Transgender ☐ Questioning			
DOB Data Quality	☐ Full DOB Reported ☐ Approximate or Partial DOB Reported ☐ Client doesn't know ☐ Client refused								
Primary Race & Secondary Race	<u>Pri Sec</u> ☐ ☐ American Indian, or Alaska Native, or Indigenous ☐ ☐ Asian or Asian American ☐ ☐ Black, or African American, or African ☐ ☐ Native Hawaiian or Pacific Islander ☐ ☐ White ☐ ☐ Client doesn't know ☐ ☐ Client refused			Ethnicity		☐ Non-Hispanic/Non-Latin (a) (o) (x) ☐ Hispanic/Latin (a) (o) (x) ☐ Client doesn't know ☐ Client refused			
Relationship to Head of Household (HoH)	☐ Self (Head of Household) ☐ Head of Household's child ☐ Head of Household's spouse or partner ☐ Head of Household's other relation member ☐ Other (non-relation member)					Disabling Condition?		☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused	
Zip Code of Last Permanent Address				Client Location (CoC) & Current County of Service				☐ CA-516 ☐ Del Norte ☐ Lassen ☐ Modoc ☐ Plumas ☐ Shasta ☐ Sierra ☐ Siskiyou	
Zip Data Quality	☐ Full Reported ☐ Partial/Approx. Reported ☐ Client doesn't know ☐ Client refused								
NOTES:									

4. Homeless Determination				
Prior Living Situation Where did you spend last night? <i>(all adults & unaccompanied youth)</i>	--HOMELESS SITUATION-- ☐ Place not meant for human habitation (car, abandoned building, bus or train station, etc.) ☐ Emergency shelter (incl. hotel/motel or campground paid for w/ES voucher, or RHY-funded Host Home Shelter) (ES) ☐ Safe Haven (SH) --INSTITUTIONAL SITUATIONS-- ☐ Foster care home or foster care group home ☐ Hospital or other residential non-psychiatric medical facility ☐ Jail, prison, or juvenile detention facility ☐ Long-term care facility or nursing home ☐ Psychiatric hospital or other psychiatric facility ☐ Substance abuse treatment facility/detox --TEMPORARY AND PERMANENT HOUSING SITUATIONS ☐ Residential project or halfway house w/no homeless criteria ☐ Hotel or motel paid for without emergency shelter voucher ☐ Transitional housing for homeless persons (including homeless youth) * ☐ Host Home (non-crisis) ☐ Staying or living in a friend's room, apartment or house ☐ Staying or living in a family member's room, apartment or house ☐ Rental by client, with GPD TIP housing subsidy ☐ Rental by client, with VASH subsidy ☐ Permanent housing (other than RRH) for formerly homeless persons ☐ Rental by client, with RRH or equivalent subsidy ☐ Rental by client, with HCV voucher (tenant or project based) ☐ Rental by client in a public housing unit ☐ Rental by client, no ongoing housing subsidy ☐ Rental by client, with other ongoing housing subsidy ☐ Owned by client, with ongoing housing subsidy ☐ Owned by client, no ongoing housing subsidy --OTHER-- ☐ Client doesn't know ☐ Client refused ☐ Data Not Collected			
	*If yes to Transitional/Permanent Housing or Institutional Situations: On the night before, did you stay on the streets, ES or SH? ☐ Yes ☐ No			
Length of stay in previous place	☐ One night or less ☐ Two to six nights ☐ One week or more, but less than one month ☐ One month or more, but less than 90 days ☐ 90 days or more, but less than one year ☐ One year or longer ☐ Client doesn't know ☐ Client refused	Number of times client has been homeless (on the streets, in ES, or SH) in past three years including today	☐ 1 time ☐ 2 times ☐ 3 times ☐ Four or more times ☐ Client doesn't know ☐ Client refused	
Approximate date homelessness started	Month Day Year	Total number of months homeless on the street in the past three years	☐ 1 month (this time is the first month) ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ More than 12 months ☐ Client doesn't know ☐ Client refused	
5. Monthly Income				
Income from any source: ☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused				
Source of Income:	Receiving Income Source	Amount Received	Additional Household Members	Notes
Alimony or Other Spousal Support	☐ Yes ☐ No	\$	\$	
Child Support	☐ Yes ☐ No	\$	\$	
Earned Income (wages)	☐ Yes ☐ No	\$	\$	
General Assistance (GA)	☐ Yes ☐ No	\$	\$	
Other	☐ Yes ☐ No	\$	\$	
Pension or retirement income from another job	☐ Yes ☐ No	\$	\$	
Private Disability Insurance	☐ Yes ☐ No	\$	\$	
Retirement Income from Social Security	☐ Yes ☐ No	\$	\$	
SSDI	☐ Yes ☐ No	\$	\$	
SSI	☐ Yes ☐ No	\$	\$	
TANF (including CalWORKs)	☐ Yes ☐ No	\$	\$	
Unemployment Insurance	☐ Yes ☐ No	\$	\$	

VA Non-Service-Connected Disability Pension	☐ Yes ☐ No	\$	\$	
VA Service-Connected Disability Compensation	☐ Yes ☐ No	\$	\$	
Worker's Compensation	☐ Yes ☐ No	\$	\$	
6. Non-Cash Benefits				
Non-cash benefit from any source: ☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused				
Source of Non-cash benefit:	Receiving Benefit	Type Received	Additional Household Members	Notes
SNAP including CalFresh (Food Stamps)	☐ Yes ☐ No			
Special Supplemental Nutrition Program (WIC)	☐ Yes ☐ No			
TANF Child Care Services	☐ Yes ☐ No			
TANF Transportation Services	☐ Yes ☐ No			
Other TANF Funded Services (Sec.8/Public Housing/Rent Assist)	☐ Yes ☐ No			
Other Source	☐ Yes ☐ No			
7. Health Insurance				
Covered by Health Insurance: ☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused				
Health Insurance type:	Covered?	Start date	Insurance Notes	
MEDICAID/MEDI-CAL	☐ Yes ☐ No			
MEDICARE	☐ Yes ☐ No			
State Children's Health Insurance Program	☐ Yes ☐ No			
Veteran's Administration (VA) Medical Services	☐ Yes ☐ No			
Employer – Provided Health Insurance	☐ Yes ☐ No			
Health Insurance obtained through COBRA	☐ Yes ☐ No			
Private Pay Health Insurance	☐ Yes ☐ No			
State Health Insurance for Adults	☐ Yes ☐ No			
Indian Health Services Program	☐ Yes ☐ No			
Other	☐ Yes ☐ No			
8. Disabilities				
Disability Type:	Disability Determination	If Yes, Expected to be of long- continued and indefinite duration and substantially impairs ability to live independently?	Start date	Disability Notes
Alcohol Use Disorder	☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused	☐ Yes ☐ Client doesn't know ☐ No ☐ Client refused		
Both Alcohol and Drug Use Disorder	☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused	☐ Yes ☐ Client doesn't know ☐ No ☐ Client refused		
Chronic Health Condition	☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused	☐ Yes ☐ Client doesn't know ☐ No ☐ Client refused		
Developmental	☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused	☐ Yes ☐ Client doesn't know ☐ No ☐ Client refused		
Drug Use Disorder	☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused	☐ Yes ☐ Client doesn't know ☐ No ☐ Client refused		
HIV/AIDS	☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused	☐ Yes ☐ Client doesn't know ☐ No ☐ Client refused		
Mental Health Disorder	☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused	☐ Yes ☐ Client doesn't know ☐ No ☐ Client refused		
Physical	☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused	☐ Yes ☐ Client doesn't know ☐ No ☐ Client refused		

9. Domestic Violence Questions			
Are you a Domestic Violence Victim/Survivor?		☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused	
IF YES – When did the Domestic Violence experience occur?		☐ Within past 3 months ☐ 3-6 mo. Ago ☐ 6-12 mo. Ago ☐ More than a year ago ☐ Client doesn't know ☐ Client refused	
		IF YES – Are you currently fleeing? ☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused	
10. Coordinated Entry Questions			
Do you have a felony conviction?		☐ Yes ☐ No	Registered sex offender? ☐ Yes ☐ No
Have you ever been denied housing because of criminal convictions?		☐ Yes ☐ No	Do you have any pets? ☐ Yes ☐ No
11. Residential Move-In Date			
If Yes, Date of Move-In	Month Day Year		
NOTES:			

Appendix J: Minor Intake Form

NorCal HMIS Minor Intake Form

Please fill out (1) form for each child

Agency Case No:			Service Point Client No:			
1. Head of Household Information						
Intake Date	Mont	ay	Year	Name of HOH:		
	SSN:			DOB:		
2. Household Relationship						
Relationship to Head of Household	☐ Brother	☐ Granddaughter	☐ Nephew	☐ Son		
	☐ Daughter	☐ Grandfather	☐ Niece	☐ Son-in-law		
	☐ Daughter-in-law	☐ Grandmother	☐ Other non-relative	☐ Step-daughter		
	☐ Father	☐ Grandson	☐ Other relative	☐ Step-son		
	☐ Father-in-law	☐ Husband	☐ Self	☐ Unknown		
	☐ Foster daughter	☐ Mother	☐ Significant other	☐ Wife		
☐ Foster son	☐ Mother-in-law	☐ Sister				
3. Client Information						
First		Middle		Last		
Alias						
SSN	- -		Gender	☐ Male ☐ Female ☐ A gender other than singularly female or male (e.g., non-binary, genderfluid, agender, culturally specific gender). ☐ Transgender ☐ Questioning		
SSN Data Quality	☐ Full Reported ☐ Partial/Approx. Reported ☐ Client doesn't know ☐ Client refused					
Date of Birth	Month	Day	Year	Ethnicity	☐ Non-Hispanic/Non-Latin (a) (o) (x) ☐ Hispanic/Latin (a) (o) (x) ☐ Client doesn't know ☐ Client refused	
DOB Data Quality	☐ Full Reported ☐ Partial/Approx. Reported ☐ Client doesn't know ☐ Client refused					
Primary Race & Secondary Race	Pri Sec ☐ ☐ American Indian, Alaska Native, or Indigenous ☐ ☐ Asian, or Asian American ☐ ☐ Black, African American, or African ☐ ☐ Native Hawaiian or Pacific Islander ☐ ☐ White ☐ ☐ Client doesn't know ☐ ☐ Client refused			Disabling Condition?	☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused	
Zip Code of Last Permanent Address						
			Zip Data Quality	☐ Full Reported ☐ Partial/Approx. Reported ☐ Client doesn't know ☐ Client refused		
4. Monthly Income/Non-Cash Benefits/Health Insurance/Disabilities						
Income from any source:			☐ Yes ☐ No <i>(If yes, Please record on HoH Intake.)</i>			
Covered by Health Insurance:			☐ Yes ☐ No ☐ Client doesn't know ☐ Client refused			
Health Insurance Type:	☐ MEDICAID/MEDI-CAL ☐ MEDICARE ☐ State Children's Health Insurance Program ☐ VA Medical Services ☐ Employer – Provided Health Insurance ☐ Health Insurance obtained through COBRA ☐ Private Pay Health Insurance ☐ State Health Insurance for Adults ☐ Indian Health Services Program ☐ Other					
Disability Type:	Determination	If Yes, Expected to be of long-continued and indefinite duration and substantially impairs ability to live independently?				
Alcohol Use Disorder	☐ Yes ☐ No	Start Date:	☐ Yes	☐ No	☐ Client doesn't know ☐ Client refused	
Both Alcohol and Drug Use Disorder	☐ Yes ☐ No	Start Date:	☐ Yes	☐ No	☐ Client doesn't know ☐ Client refused	
Chronic Health Condition	☐ Yes ☐ No	Start Date:	☐ Yes	☐ No	☐ Client doesn't know ☐ Client refused	
Developmental	☐ Yes ☐ No	Start Date:	☐ Yes	☐ No	☐ Client doesn't know ☐ Client refused	
Drug Abuse	☐ Yes ☐ No	Start Date:	☐ Yes	☐ No	☐ Client doesn't know ☐ Client refused	
HIV/AIDS	☐ Yes ☐ No	Start Date:	☐ Yes	☐ No	☐ Client doesn't know ☐ Client refused	
Mental Health Disorder	☐ Yes ☐ No	Start Date:	☐ Yes	☐ No	☐ Client doesn't know ☐ Client refused	
Physical	☐ Yes ☐ No	Start Date:	☐ Yes	☐ No	☐ Client doesn't know ☐ Client refused	

*Please make sure to get a RELEASE OF INFORMATION (ROI) signed for each additional adult Household member. *

Appendix K: Exit Form – all household members

1. Exit Summary		
Agency Name		Staff Name
Program Name		Staff Phone Line
Date of entry into program		Date of exit from program
2. Client Information		
Client Name		Today's Date
SSN		Street Address
Date of Birth		City, State, Zip
Email		Phone
3. Reason For Leaving		
	☐ Completed program ☐ Criminal activity/violence ☐ Death ☐ Disagreement with rules/persons ☐ Left for housing opportunity before completing program ☐ Needs could not be met ☐ Non-compliance with program ☐ Non-payment of rent ☐ Other ☐ Reached maximum time allowed ☐ Unknown/Disappeared	
If other, specify:		
4. Destination		
	HOMELESS SITUATION ☐ Place not meant for habitation ☐ Emergency shelter, including hotel or motel paid for with emergency shelter voucher ☐ Safe Haven INSTITUTIONAL SITUATIONS ☐ Foster care home or foster care group home ☐ Hospital or other residential non-psychiatric medical facility ☐ Jail, prison, or juvenile detention facility ☐ Long-term care facility or nursing home ☐ Psychiatric hospital or other psychiatric facility ☐ Substance abuse treatment facility or detox center TEMPORARY AND PERMANENT HOUSING SITUATIONS ☐ Residential project or halfway house w/no homeless criteria ☐ Hotel or motel paid for without emergency shelter voucher ☐ Transitional housing for homeless persons (including homeless youth) * ☐ Host Home (non-crisis) ☐ Staying or living in a friend's room, apartment or house, temporary tenure ☐ Staying or living in a family member's room, apartment or house, temporary tenure ☐ Staying or living in a friend's room, apartment or house, permanent tenure ☐ Staying or living in a family member's room, apartment or house, permanent tenure ☐ Moved from one HOPWA funded project to HOPWA PH ☐ Moved from one HOPWA funded project to HOPWA TH ☐ Rental by client, with GPD TIP housing subsidy ☐ Rental by client, with VASH housing subsidy ☐ Permanent housing (other than RRH) for formerly homeless persons ☐ Rental by client, with RRH or equivalent subsidy ☐ Rental by client, with HCV voucher (tenant or project based) ☐ Rental by client in a public housing unit ☐ Rental by client, no ongoing housing subsidy ☐ Rental by client, with other ongoing housing subsidy ☐ Owned by client, with ongoing housing subsidy ☐ Owned by client, no ongoing housing subsidy OTHER ☐ No exit interview completed ☐ Other ☐ Deceased ☐ Client doesn't know ☐ Client refused ☐ Data Not Collected	
If other, specify:		
5. Residential Move-In Date		
If Yes, Date of Move-In	Month	Day Year

6. Updates			
Monthly Income	Amount	Non-Cash Benefits	Amount
☐ NO CHANGE AT EXIT		☐ NO CHANGE AT EXIT	
☐ Alimony or Other Spousal Support	\$	☐ SNAP including CalFresh (Food Stamps)	\$
☐ Child Support	\$	☐ Special Supplemental Nutrition Program (WIC)	\$
☐ Earned Income (wages)	\$	☐ TANF Child Care Services	\$
☐ General Assistance (GA)	\$	☐ TANF Transportation Services	\$
☐ Other	\$	☐ Other TANF Funded Services (Sec.8/Public Housing/Rent Assist)	\$
☐ Pension or retirement income from another job	\$	☐ Other Source	\$
☐ Private Disability Insurance	\$		
☐ Retirement Income from Social Security	\$		
☐ SSDI	\$		
☐ SSI	\$		
☐ TANF (including CalWORKs)	\$		
☐ Unemployment Insurance	\$		
☐ VA Non-Service-Connected Disability Pension	\$		
☐ VA Service-Connected Disability Compensation	\$		
☐ Worker's Compensation	\$		
Health Insurance:	Notes	Disabilities	Notes
☐ NO CHANGE AT EXIT		☐ NO CHANGE AT EXIT	
☐ MEDICAID/MEDI-CAL		☐ Alcohol Abuse	
☐ MEDICARE		☐ Both Alcohol and Drug Abuse	
☐ State Children's Health Insurance Program		☐ Chronic Health Condition	
☐ Veteran's Administration (VA) Medical Services		☐ Developmental	
☐ Employer – Provided Health Insurance		☐ Drug Abuse	
☐ Health Insurance obtained through COBRA		☐ HIV/AIDS	
☐ Private Pay Health Insurance		☐ Mental Health Problem	
☐ State Health Insurance for Adults		☐ Physical	
☐ Indian Health Services Program			
☐ Other			

*****OPTIONAL EXIT QUESTIONS*****

What supportive services did the client receive while in the program?

☐ Outreach	☐ Education
☐ Drug or Alcohol abuse services	☐ Childcare
☐ Employment assistance	☐ Domestic Violence services
☐ Legal Services	☐ Life skills (outside of case management)
☐ Credit repair	☐ Housing placement and search
☐ Medi-Cal related services	☐ Transportation
☐ Case management	☐ Financial Assistance
☐ Mental Health services	☐ Other
☐ Landlord engagement	



HMIS PRIVACY & SECURITY PLAN

NorCal CA 516
Homeless Continuum of Care

2021

PRIVACY & SECURITY

Privacy refers to the protection of the client's data stored in an HMIS from open view, sharing, inappropriate use, or unauthorized disclosure. Security refers to the protection of the client's data stored in the HMIS from unauthorized access, use, disclosure, or modification.

Contents

Introduction	2
Privacy	2
Privacy Plan Overview	2
HMIS User Responsibilities	3
Agency Responsibilities	3
System Security	6
Security Plan Overview	6
Security Plan Applicability	6
Security Officers	6
Lead Security Officer	6
Participating Agency Security Officer	6
Physical Safeguards	7
Technical Safeguards	7
Workstation Security	7
Establishing HMIS User IDs and Access Levels	7
User Authentication	8
Rescinding User Access	8
Disposing Electronic, Hardcopies, Etc	10
Other Technical Safeguards	9
Disaster Recovery Plan	9
Workforce Security	10
Reporting Security Incidents	10
Privacy and Security Monitoring	11
New HMIS Participating Agency Site Security Assessment	11
Annual Security Audits	13
Attachment A: Security Checklist	14

Introduction

The HMIS System Administrator is responsible for overseeing HMIS privacy and security. The HMIS System Administrator may delegate some specific duties related to maintaining HMIS privacy and security to an HMIS System Administrator. HMIS Participating Agencies are responsible for preventing degradation of the HMIS resulting from viruses, intrusion, or other factors within the agency's control and for preventing inadvertent release of confidential client- specific information through physical, electronic or visual access to End User workstations. Each Participating Agency is responsible for ensuring it meets the Privacy and Security requirements detailed in the HUD HMIS Data and Technical Standards. Participating Agencies will conduct a thorough review of internal policies and procedures regarding HMIS annually.

Privacy

Privacy Plan Overview

On July 30, 2004, the US Department of Housing and Urban Development (HUD) released the Data and Technical standards for Homeless Management Information Systems (Federal Register, Vol. 69, No.146-45888) and on December 9, 2011 HUD released [HMIS Requirements Proposed Rule \(Federal Register / Vol. 76, No. 237\)](#).

These standards outlined the responsibilities of the HMIS and for the agencies which participate in an HMIS. This section describes the Privacy Plan of the NorCal CA 516 Homeless Continuum of Care HMIS. All users, agencies and system administrators must adhere to this Privacy Plan.

We intend our Privacy Plan to support our mission of providing an effective and usable case management tool. We recognize that clients served by individual agencies are not exclusively that "agency's client" but instead are truly a client of the NorCal CA 516 Continuum of Care. Thus, we have adopted a Privacy Plan which supports an open system of client-level data sharing among agencies. The data is owned by the NorCal CA 516 CoC that is entered into the NorCal HMIS; and the clients own their own personal data.

The core tenet of our Privacy Plan is the Baseline Privacy Statement. The Baseline Privacy Statement describes how client information may be used and disclosed and how clients can get access to their information. Each agency must either adopt the Baseline Privacy Statement or develop a Privacy Statement which meets and exceeds all minimum requirements set forth in the Baseline Privacy Statement (this is described in the Participating Agency Responsibilities section of this Privacy Plan). This ensures that all agencies who participate in the HMIS are governed by the same minimum standards of client privacy protection.

Baseline Privacy Statement: This is the main document of this Privacy Plan. This document outlines the minimum standard by which an agency collects, utilizes, and discloses information.	*REQUIRED* Participating Agencies must adopt a privacy statement which meets all minimum standards and to post this Statement on your Agency's local website (if available).
Consumer Notice Posting: This posting explains the reason for asking for personal information and notifies the client of the Privacy Notice.	*REQUIRED* Agencies must adopt and utilize a Consumer Notice Posting.

HMIS Client Consent Form: This form must be signed by all adult clients and unaccompanied youth. This gives the client the opportunity to refuse the sharing of their information to other agencies within the system.	*REQUIRED* Client Signatures are required to share with participating agencies.
---	--

HMIS User Responsibilities

A client's privacy must be upheld by the users and direct service providers and can also be made public at the client's discretion. The role and responsibilities of the user cannot be over-emphasized. A user is defined as a person that has direct interaction with a client or their data. (This could potentially be any person at the agency: staff member, volunteer, contractor, etc.)

Users have the responsibility to:

- Understand their agency's Privacy Statement;
- Be able to explain their agency's Privacy Statement to clients;
- Follow their agency's Privacy Statement;
- Know where to refer the client if they cannot answer the client's questions;
- Complete **HMIS Client Consent Form** with client prior to collecting HMIS data;
- Present their agency's Privacy Statement and the HMIS Notice of Privacy Practices to the client before collecting any information; and
- Uphold the client's privacy in HMIS.

Agency Responsibilities

The 2004 HUD HMIS Data and Technical Standards emphasize that it is the Participating Agency's responsibility for upholding client privacy. All agencies must take this task seriously and take time to understand the legal, ethical and regulatory responsibilities. This Privacy Plan and the Baseline Privacy Statement provide guidance on the minimum standards by which agencies must operate if they wish to participate in the HMIS.

Meeting the minimum standards in this Privacy Plan and the Baseline Privacy Statement are required for participation in HMIS. Any Participating Agency may exceed the minimum standards described and are encouraged to do so.

Participating Agencies have the responsibility to:

- Review their program requirements to determine what industry privacy standards must be met that exceed the minimum standards outlined in this Privacy Plan and Baseline Privacy Statement (examples: Substance Abuse Providers covered by 24 CFR Part 2, HIPAA Covered Agencies, Legal Service Providers);
- Review the 2004 HMIS Data and Technical Standards (Federal Register, Vol 69, No. 146-45888);
- Ensure that all clients are aware of the adopted Privacy Plan and have access to it.
- Make reasonable accommodations for persons with disabilities, language barriers or education barriers;
- Ensure that anyone working with clients covered by the Privacy Plan can meet the User Responsibilities; and
- Designate at least one Security Officer (May be the same as the Participating Agency HMIS Lead) that has been trained to technologically uphold the agency's adopted Privacy Plan.

Each HMIS Participating Agency must use this Privacy Plan that describes how and when the Participating Agency may use and disclose clients' Protected Identifying Information (PII). PII includes name, Social Security Number (SSN), date of birth, zip code, project entry and/or exit date, and unique personal identification number (HMIS Unique Identifier).

Participating Agencies may be required to collect some PII by law, or by organizations that give the agency money to operate their projects. PII is also collected by Participating Agencies to monitor project operations, to better understand the needs of people experiencing homelessness, and to improve services for people experiencing homelessness. Participating Agencies are permitted to collect PII only with a client's written consent.

Participating Agencies may use and disclose client PII to:

- Verify eligibility for services;
- Provide clients with and/or refer clients to services that meet their needs;
- Manage and evaluate the performance of programs;
- Report about program operations and outcomes to funders and/or apply for additional funding to support agency programs;
- Collaborate with other local agencies to improve service coordination, reduce gaps in services, and develop community-wide strategic plans to address basic human needs; and
- Participate in research projects to better understand the needs of people served. Participating

Agencies may also be required to disclose PII for the following reasons:

- When the law requires it;
- When necessary to prevent or respond to a serious and imminent threat to health or safety; and
- When a judge or law enforcement orders it.

Participating Agencies are obligated to limit disclosures of PII to the minimum necessary to accomplish the purpose of the disclosure. Uses and disclosures of PII not described above may only be made with a client's written consent. Clients have the right to revoke consent at any time by submitting a request in writing.

Clients also have the right to request in writing:

- A copy of all PII collected;
- An amendment to any PII used to make decisions about the client's care and services.
- Restrictions on the type of information disclosed to outside Participating Agencies.

Participating Agencies may reserve the right to refuse a client's request for inspection or copying of PII in the following circumstances:

- Information compiled in reasonable anticipation of litigation or comparable proceedings;
- The record includes information about another individual (other than a health care or homeless provider);
- The information was obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) and a disclosure would reveal the source of the information; and
- The Participating Agency believes that disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

If a client's request is denied, the client should receive a written explanation of the reason of the denial. The client has the right to appeal the denial by following the established Participating Agency grievance procedure. Regardless of the outcome of the appeal, the client shall have the right to add to his/her program records a concise statement of disagreement. The Participating Agency shall disclose the statement of disagreement whenever it discloses the disputed PII.

All individuals with access to PII are required to complete formal training in privacy requirements at least annually.

This document should, at a minimum, reflect the baseline requirements listed in the HUD HMIS

Data and Technical Standards Final Notice, published July 2004 and revised in March 2010. The privacy policy may be amended at any time and all amendments to the privacy notice must be consistent with the requirements of the US Department of Housing and Urban Development (HUD) Data and Technical standards for Homeless Management Information Systems (July 30, 2004, Federal Register/ Vol. 69, No. 146, 45888). If there is any instance where this Privacy Statement is not consistent with the HUD Standards, the HUD Standards take precedence. Should any inconsistencies be identified, please immediately notify the NorCal CA 516 HMIS System Administrator , using the contact information below.

All questions and requests related to this Privacy Statement should be directed to: HMIS System Administrator: email: HMIS@NorCalUnitedWay.org

HMIS System Administrator : System Administration Responsibilities

HMIS System Administrator has the responsibility to:

- Adopt and uphold a Privacy Plan which meets or exceeds all minimum standards in the Baseline Privacy Statement;
- Train and monitor all users and Security Officer upholding system privacy;
- Monitor agencies to ensure adherence to the adopted Privacy Plan; and
- Provide training to agencies and users on this Privacy Plan.

System Security

Security Plan Overview

HMIS security standards are established to ensure the confidentiality, integrity and viability of all HMIS information. The security standards are designed to protect against any reasonably anticipated threats or hazards to security and must be enforced by system administrators, agency administrators as well as end users. This section is written to comply with the 2004 Homeless Management Information Systems (HMIS) Data and Technical Standards Final Notice (Federal Register, Vol 69, No. 146-45888) as well as local legislation pertaining to maintaining an individual's personal information. Meeting the minimum standards in this Security Plan is required for participation in HMIS. Any agency may exceed the minimum standards described in this plan and are encouraged to do so. All Agency Administrators are responsible for understanding this policy and effectively communicating the Security Plan to individuals responsible for security at their agency.

Security Plan Applicability

The HMIS and all Participating Agencies must apply the security standards addressed in this Security Plan to all the systems where personal protected information is stored or accessed. Additionally, all security standards must be applied to all networked devices. This includes, but is not limited to, networks, desktops, laptops, mobile devices, mainframes and servers.

All agencies will be monitored by the HMIS System Administrators annually to ensure compliance with the Security Plan. Participating Agencies that do not adhere to the security plan will be given a reasonable amount of time to address any concerns. Egregious violations of the security plan may result in immediate termination of an agency or user's access to the HMIS as determined by the HMIS Lead.

Security Officers

The HMIS System Administrator and all HMIS Participating Agencies must designate a Security Officer to oversee HMIS privacy and security. This person will act as a single point-of-contact who is responsible for annually certifying that Participating Agencies adhere to the Security Plan and testing the CoC's security practices for compliance.

Lead Security Officer

- May be an HMIS System Administrator or another employee, volunteer or contractor designated by the HMIS System Administrator who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance;
- Assesses security measures in place prior to establishing access to HMIS for a new Agency;
- Reviews and maintains file of Participating Agency annual compliance certification checklists; and
- Conducts annual security audit of all Participating Agencies.

Participating Agency Security Officer

- May be the Participating Agency HMIS Lead or another Participating Agency employee, volunteer or contractor who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance;
- Conducts a security audit for any workstation that will be used for HMIS purposes; and
 - No less than annually for all agency HMIS workstations; AND
 - Prior to issuing a User ID to a new HMIS End User; AND
 - Any time an existing user moves to a new workstation.

- Continually ensures each workstation within the Participating Agency used for HMIS data collection or entry is adequately protected by a firewall and antivirus software (per Technical Safeguards – [Workstation Security](#)).

Upon request, the HMIS System Administrator may be available to provide Security support to Participating Agencies who do not have the staff capacity or resources to fulfill the duties assigned to the Participating Agency Security Officer.

Physical Safeguards

In order to protect client privacy, it is important that the following physical safeguards be put in place. For the purpose of this section, authorized persons will be considered only those individuals who have completed Privacy and Security training within the past 12 months.

- Computer Location – A computer used as an HMIS workstation must be in a secure location where only authorized persons have access. The workstation must not be accessible to clients, the public or other unauthorized Participating Agency staff members or volunteers. A password protected automatic screen saver will be enabled on any computer used for HMIS data entry.
- Printer location – Documents printed from HMIS must be sent to a printer in a secure location where only authorized persons have access.
- PC Access (visual) — Non-authorized persons should not be able to see an HMIS workstation screen. Monitors should be turned away from the public or other unauthorized Participating Agency staff members or volunteers and utilize visibility filters to protect client privacy.
- Mobile Device – A mobile device used to access and enter information into the HMIS must use a password or other user authentication on the lock screen to prevent an unauthorized user from accessing it and it should be set to automatically lock after a set period of device inactivity. A remote wipe and/or remote disable option should also be downloaded onto the device.

Technical Safeguards

Workstation Security

- To promote the security of HMIS and the confidentiality of the data contained therein, access to HMIS will be available only through approved workstations.
- Participating Agency Security Officer will confirm that any workstation accessing HMIS shall have antivirus software with current virus definitions (updated at minimum every 24 hours) and frequent full system scans (at minimum weekly).
- Participating Agency Security Officer will confirm that any workstation accessing HMIS has and uses a hardware or software firewall; either on the workstation itself if it accesses the internet through a modem or on the central server if the workstation(s) accesses the internet through the server.

Establishing HMIS User IDs and Access Levels

- The HMIS System Administrator, in conjunction with the Participating Agency HMIS Lead, will ensure that any prospective Participating Agency End User reads, understands and signs the HMIS End User Agreement annually. The HMIS System Administrator will maintain a file of all signed HMIS End User Agreements.
- The Participating Agency HMIS Security Officer is responsible for ensuring that all Participating Agency End Users have completed mandatory trainings, including HMIS Privacy, Security and Ethics training and Participating Agency End User Responsibilities and Workflow training, prior to being provided with a User ID to access HMIS. Participating Agency End-Users must review and sign an HMIS End User Agreement with the HMIS Administrator on an annual basis.

- All Participating Agency End Users will be issued a unique User ID and password. Sharing of User IDs and passwords by or among more than one Participating Agency End User is expressly prohibited. Each Participating Agency End User must be specifically identified as the sole holder of a User ID and password. User IDs and passwords may not be transferred from one user to another.
- The HMIS System Administrator will always attempt to assign the most restrictive access that allows a Participating Agency End User to efficiently and effectively perform his/her duties.
- The HMIS System Administrator will create the new User ID and notify the User ID owner of a temporary password.
- When the Participating Agency determines that it is necessary to change a user's access level, the HMIS System Administrator will update the user's access level as needed.

User Authentication

- User IDs are individual, and passwords are confidential. No individual should ever use or allow use of a User ID that is not assigned to that individual, and user- specified passwords should never be shared or communicated in any format.
- Temporary passwords must be changed on first use. User-specified passwords must be a minimum of 8 characters long and must contain a combination of upper case and lower-case letters, a number and a symbol.
- Participating Agency End users will be prompted by the software to change their password every 90 days.
- Participating Agency End Users must immediately notify the HMIS System Administrator if they have reason to believe that someone else has gained access to their password.
- Three consecutive unsuccessful attempts to login will disable the User ID until the password is reset. For Participating Agency End Users, passwords can be reset by the HMIS System Administrator or directly on ServicePoint's website log in page with the "forgot password" link.
- Users must log out from the HMIS application and either lock or log off their respective workstation if they leave. If the user logged into HMIS and the period of inactivity in HMIS exceeds 30 minutes, the user will be logged off the HMIS automatically.

Rescinding User Access

- The Participating Agency will notify the HMIS System Administrator as soon as possible, but not later than 3 business days if a Participating Agency End User no longer requires access to perform his or her assigned duties due to a change of job duties or termination of employment or any other valid reason.
- The HMIS System Administrator reserves the right to terminate Participating Agency End User licenses that are inactive for 90 days or more. All end users that have been deactivated for 6 months or more must attend additional training.
- In the event of suspected or demonstrated noncompliance by a Participating Agency End User with the HMIS Participating Agency End User Agreement or any other HMIS plans, forms, standards or governance documents, the Participating Agency Security Officer shall notify the HMIS System Administrator to deactivate the User ID for the Participating Agency End User in question until an internal agency investigation has been completed. The HMIS System Administrator should be notified of any substantiated incidents that may have resulted in a breach of HMIS system security and/or client confidentiality, whether or not a breach is definitively known to have occurred.
- Any agency personnel who are found to have misappropriated client data (identity theft, releasing personal client data to any unauthorized party), shall have HMIS privileges revoked.
- The Continuum of Care is empowered to permanently revoke a Participating Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the

NorCal CA 516 Homeless Continuum of Care HMIS Policies and Procedures, or the HMIS Privacy Statement that resulted in a release of PII.

Disposing Electronic, Hardcopies, Etc.

- Computer: All technology equipment (including computers, printers, copiers and fax machines) used to access HMIS and which will no longer be used to access HMIS will have their hard drives reformatted multiple times. If the device is now non-functional, it must have the hard drive sanitized by a method current to industry standards.
- Hardcopies: For paper records, shredding, burning, pulping, or pulverizing the records so that PII is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
- Mobile Devices: Use software tools that will thoroughly delete/wipe all information on the device and return it to the original factory state before discarding or reusing the device.

Other Technical Safeguards

- Unencrypted PII may not be stored or transmitted in any fashion—including sending file attachments by email or downloading reports including PII to a flash drive, to the End User's desktop or to an agency shared drive unless the reports or documents containing PII are password protected or stored on a hard drive that is password protected with an enabled password protected screen saver.

Disaster Recovery Plan

Disaster recovery for the NorCal CA 516 HMIS will be conducted by the HMIS System Administrator with support from the HMIS software vendor as needed. The HMIS System Administrator must be familiar with the disaster recovery plan set in place by the HMIS software vendor.

- WellSky Disaster Recovery Plan:
 - Contact information – email: BOW-support@wellsky.com; .
 - Phone Number: 1-844-216-8780
 - It includes:
 - Nightly database backups.
 - Offsite storage of backups
 - 7-day backup history stored locally on instantly accessible RAID storage
 - 1-month backup history stored off site
 - 24 x 7 access to WellSky's emergency line to provide assistance related to "outages" or "downtime".
 - 24 hours backed up locally on instantly-accessible disk storage
 - All customer site databases are stored online, and are readily accessible for approximately 24 hours; backups are kept for approximately one (1) month. Upon recognition of a system failure, a site can be copied to a standby server, and a database can be restored, and site recreated within three (3) to four (4) hours if online backups are accessible. As a rule, a site restoration can be made within six (6) to eight (8) hours. On-site backups are made once daily and a restore of this backup may incur some data loss between when the backup was made and when the system failure occurred.
 - All internal servers are configured in hot-swappable hard drive RAID configurations. All systems are configured with hot-swappable redundant power supply units. Our Internet connectivity is comprised of a primary and secondary connection with separate internet service providers to ensure redundancy in the event of an ISP connectivity outage. The primary Core routers are configured with redundant power supplies, and are configured in tandem so that if one core router fails the secondary router will continue operation with little to no interruption in service. All servers, network devices, and related hardware are powered via APC Battery Backup units that

in turn are all connected to electrical circuits that are connected to a building generator.

-
- All client data is backed-up online and stored on a central file server repository for 24 hours. Each night an encrypted backup is made of these client databases and secured in an offsite datacenter.
- Historical data can be restored from backups as long as the data requested is 30 days or newer. As a rule, the data can be restored to a standby server within 6-8 hours without affecting the current live site. Data can then be selectively queried and/or restored to the live site.
- For power outage, our systems are backed up via APC battery back-up units, which are also in turn connected via generator-backed up electrical circuits. For a system crash, Non-Premium Disaster Recovery Customers can expect six (6) to eight (8) hours before a system restore with potential for some small data loss (data that was entered between the last backup and when the failure occurred) if a restore is necessary. If the failure is not hard drive related these times will possibly be much less since the drives themselves can be repopulated into a standby server.
- All major outages are immediately brought to the attention of executive management. WellSky support staff helps manage communication or messaging to customers as progress is made to address the service outage. WellSky takes major outages seriously, understands, and appreciates that the customer becomes a tool and utility for daily activity and client service workflow.
- All HMIS Participating Agency HMIS Leads should be aware of and trained to complete any tasks or procedures for which they are responsible at their agency in the event of a disaster, to include maintain a contact list with account number of the Vendor, Agencies, and their Internal IT Department.

Workforce Security

Reporting Security Incidents

These Security Standards and the associated HMIS Policies and Procedures are intended to prevent, to the greatest degree possible, any security incidents. However, should a security incident occur, the following procedures should be followed in reporting:

- Any HMIS Participating Agency End User who becomes aware of or suspects that HMIS system security and/or client privacy has been compromised must immediately report the concern to the Participating Agency HMIS Lead or the HMIS Administrator.
- In the event of a suspected security or privacy concern the Participating Agency HMIS Lead should complete an internal investigation. If the suspected security or privacy concern resulted from a Participating Agency End User's suspected or demonstrated noncompliance with the HMIS End User Agreement, the Participating Agency HMIS Lead should have the HMIS System Administrator deactivate the Participating Agency End User's User ID until the internal investigation has been completed.
- Following the internal investigation, the Participating Agency HMIS Lead shall notify the HMIS Administrator of any substantiated incidents that may have compromised HMIS system security and/or client privacy whether or not a release of client Personally Identifiable Information (PII) is definitively known to have occurred. If the security or privacy concern resulted from demonstrated noncompliance by an End User with the HMIS End User Agreement, the HMIS Administrator reserves the right to permanently deactivate the User ID for the End User in question.
- Within one business day after the HMIS Administrator receives notice of the security or privacy concern, the HMIS Administrator and Participating Agency HMIS Lead will jointly establish an action plan to analyze the source of the security or privacy concern and actively prevent such future concerns. The action plan shall be implemented as soon as possible, and to not exceed

implementation by thirty (30) days.

- If the Participating Agency is not able to meet the terms of the action plan within the time allotted, the HMIS System Administrator, in consultation with the NorCal Continuum of Care Advisory Board, may elect to terminate the Participating Agency's access to HMIS. The Participating Agency may appeal to the CoC Advisory Board for reinstatement to HMIS following completion of the requirements of the action plan.
- In the event of a substantiated release of PII in noncompliance with the provisions of these Security Standards, or the NorCal CA 516 HMIS Policies and Procedures, the Participating Agency HMIS Lead will make a reasonable attempt to notify all impacted individual(s). The HMIS Administrator must approve of the method of notification and the Participating Agency HMIS Lead must provide the HMIS Administrator with evidence of the Participating Agency's notification attempt(s). If the HMIS Administrator is not satisfied with the Participating Agency's efforts to notify impacted individuals, the HMIS Administrator will attempt to notify impacted individuals at the Agency's expense.
- The HMIS System Administrator will notify the appropriate body of the Continuum of Care of any substantiated release of PII in noncompliance with the provisions of these Security Standards, the HMIS Policies and Procedures
- The HMIS System Administrator will maintain a record of all substantiated releases of PII in noncompliance with the provisions of these Security Standards, or the NorCal CA 516 HMIS Policies and Procedures for 7 years.

The Continuum of Care reserves the right to permanently revoke a Participating Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, or the NorCal CA 516 HMIS Policies and Procedures that resulted in a release of PII

Privacy and Security Monitoring

New HMIS Participating Agency Site Security Assessment

- Prior to establishing access to HMIS for a new Participating Agency, the HMIS Administrator or designee of the HMIS/CEP Committee will review the requirements. The Participating Agency's Security Officer is responsible for ensuring information security compliance within their Agency. Each Agency's security will be evaluated through an annual security audit performed by the HMIS Administrator or designee of the HMIS/CEP Committee.
 - The HMIS System Administrator or a designee will notify the Participating Agency's Executive Director and/or Participating Agency HMIS Lead of an upcoming review.
 - The security review may be carried out by 3 different methods: (1) A Peer Review i.e. one agency reviewing another agency; (2) A Committee Member from another participating agency; or (3) HMIS/CEP Committee designee.
 - The HMIS Administrator or a designee will use the Compliance Certification Checklist to conduct security audits.
 - A random audit of the workstations used for HMIS data entry for each HMIS Participating Agency must be conducted. In the event that an agency has more than 1 project site, each project site must be audited.
 - The areas of noncompliance to the NorCal CA 516 HMIS Policies and Procedures will be identified on the Security Checklist. The Participating Agency and HMIS System Administrator will work to resolve the action item(s) within 15 days.
 - Any Security Checklist that includes 1 or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved and the findings, action items, and resolution summary has been reviewed and signed by the Participating Agency's Executive Director or other empowered officer and forwarded to the HMIS System Administrator.

Attachment A: Security Checklist

Annual Security Checklist Workstation Security Standards

HMIS Participating Agency	Inspection Officer:
	Date:

This Compliance Certification is to be completed annually by peer review or by a committee member from another participating agency or by HMIS/CEP Committee designee. Every agency workstation used for HMIS data collection, data entry or reporting must be evacuated. Attach additional copies of any page of this checklist as needed. Any compliance issues identified must be resolved within 30 days. Upon completion, a copy of this checklist shall be forwarded to the HMIS System Administrator. This original checklist should be readily available on file at the HMIS Participating Agency for 7 years.

For the purpose of this section, authorized persons will be considered only those individuals who have current HMIS license and data collection authorization.

User Name:

1. The Mandatory Collection Notice is posted in an area where HMIS intake is completed and The Notice of Privacy Practices is available at the workstation. 2. HMIS workstation computer is in a secure location where only authorized persons have access. 3. HMIS workstation computer is password protected and locked when not in use. 4. Documents printed from HIMS are sent to a printer in a secure location where only authorized persons have access.	User 1.	User 2.	User 3.	User 4.	User 5.	
						<u>Notes:</u>
						<u>Notes:</u>
						<u>Notes:</u>
						<u>Notes:</u>

5. Non-authorized persons are unable to see the HMIS workstation computer monitor.

					<u>Notes:</u>
--	--	--	--	--	---------------

6. HMIS workstation computers have current antivirus software and firewall security.

7. Hard copies of PII (Client files, intake forms, printed reports. etc..) are stored in a secure location.

8. Password is kept physically secure.

9. Random audit of at least 2 HMIS client files.

User 1.	User 2.	User 3.	User 4.	User 5.	
					<u>Notes:</u>
					<u>Notes:</u>
					<u>Notes:</u>
					<u>Notes:</u>

#	Workstation Security Compliance Issues Identified	Steps taken to resolve workstation security compliance issue

Security Officer Certifications: Please initial next to each of the following statements:

_____ I have verified that All participating Agency End Users are using the most current of the HMIS Client Consent Form (ROI),

_____ The HMIS intake Form and the Notice of Privacy Practices.

Participating Agency Security Office Signature	Date	Executive Director(or designee) Signature	Date
--	------	---	------

Draft 2/19/25 NorCal Advanced Entry (2025) Assessment Question List

			Description
1 ▼	  		Date of Birth
2 ▼	  		Date of Birth Type
3 ▼	  		Gender
4 ▼	  		If Other Gender, specify
5 ▼	  		Race and Ethnicity
6 ▼	  		Additional Race and Ethnicity Detail
7 ▼	  		Relationship to Head of Household
8 ▼	  		Enrollment CoC
9 ▼	 		Prior Living Situation
10 ▼	 		Rental Subsidy Type
11 ▼	 		Length of Stay in Previous Place
12 ▼	 		Did you stay less than 90 days?
13 ▼	 		Did you stay less than 7 nights?
14 ▼	 		On the night before did you stay on the streets, ES or SH?
15 ▼	 		Approximate date this episode of homelessness started
16 ▼	 		Regardless of where they stayed last night - Number of times the client has been on the streets, in ES, or SH in the past three years including today
17 ▼	 		Total number of months homeless on the street, in ES or SH in the past three years
18 ▼	  		Does the client have a disabling condition?
19 ▼	 		Registered sex offender (any household members)
20 ▼	  		Current Living Situation - Required
21 ▼	  		Please do not forget to fill out the VI-SPDAT form! Click on Save and then select it at the top of the assessment.
22 ▼	 		Translation Assistance Needed
23 ▼	 		Preferred Language
24 ▼	 		Required response when selecting Different Preferred Language
25 ▼	 		If Different Preferred Language, please specify