MARIN COUNTY CONTINUUM OF CARE

HOMELESS MANAGEMENT INFORMATION SYSTEM POLICIES AND PROCEDURES

November 2019

I. COUNTY RESPONSIBILITIES

Marin County as the HMIS Lead Agency:

1. Will provide the Agency HMIS access via a third party software vendor, Bitfocus, via agency provided internet connection. Bitfocus's software Clarity is a web-based case management system with an HMIS component.
2. May at its sole discretion provide for a limited number of user licenses to each participating HMIS agency.
3. Will sign a Memorandum of Understanding with each participating HMIS agency.
4. Will provide client Release of Information forms to be used by individual agencies wishing to share data in HMIS.
5. Will provide Agency User Agreements to be signed by all users of the HMIS software prior to collecting or handling client data. The privacy agreement lists the privacy and confidentiality provisions the end user will abide by.
6. Will provide model Privacy Notices, data collection forms, and other templates for HMIS that may be adopted or adapted by individual agencies.
7. Will provide both initial training and periodic updates to that training for key Agency Staff regarding the use of the HMIS, with the expectation that the Agency will take responsibility for conveying this information to all Agency Staff using the system.
8. Will provide basic user support and technical assistance for the HMIS module Clarity (i.e., general trouble-shooting and assistance with standard report generation). Access to this basic technical assistance will normally be available from 6:00 AM. to 5:00 PM. on Monday through Friday (with the exclusion of holidays).
9. Ensure that the software vendor updates the system to maintain compliance with the HUD Data and Technical Standards.
10. Run aggregate reports for the purpose of planning and reporting to funders.
11. Will not publish reports on client data that identify specific agencies or persons, without prior agency (and where necessary, client) permission. Public reports otherwise published will be limited to presentation of aggregated data within the HMIS database.
12. Annually report to HUD for Longitudinal Systems Analysis, Sheltered Point in Time Count, Housing Inventory Count, and Consolidated Plan as part of the McKinney Vento funding application.
13. Will produce quarterly aggregate reports and analysis.

Marin County responsibilities may also be found in the CoC-HMIS Governance Charter.

II. AGENCY RESPONSIBILITIES

The Agency as a contributor to HMIS:

1. Will designate an agency administrator as the point of contact for HMIS related matters within the agency.
2. Will use HMIS to report to HUD as and when required.
3. Will assure that privacy and security requirements are met as detailed in the HUD HMIS Data and Technical Standards.
4. Will annually conduct a thorough review of internal policies and procedures regarding HMIS.
5. Will assure that agency end users are properly trained and sign End User agreements.
6. Will be responsible for maintaining user IDs for the HMIS system for the agency.
7. Will ensure internet connectivity.

8. Will maintain the agency data in the HMIS.
9. Will safeguard the privacy of client information.
10. Will sign a Memorandum of Understanding with the HMIS Lead Agency.
11. Will ensure that all HMIS users sign the End User privacy agreement prior to accessing any HMIS data.
12. Will ensure that all HMIS user receive yearly security and privacy training as required by HUD.

Agency responsibilities may also be found in the CoC-HMIS Governance Charter.

III. PRIVACY AND CONFIDENTIALITY

COMPLIANCE WITH FEDERAL AND STATE LAWS

1. The Agency will comply with all relevant Federal and California State laws and regulations that protect client records and privacy. Agency's duties under this provision include, but are not limited to, complying with the following:
    A. The Federal confidentiality rules as contained in the Code of Federal Regulations (CFR) 42, Part 2 Confidentiality of Alcohol and Drug Abuse Patient Records, regarding disclosure of alcohol and/or drug abuse records. In general terms, the Federal regulation prohibits the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by CFR 42, Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Agency understands that the Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.
    B. The Health Insurance Portability and Accountability Act of 1996 and corresponding regulations passed by the U.S. Department of Health and Human Services. In general, the regulations provide consumers with new rights to control the release of medical information, including advance consent for most disclosures of health information, the right to see a copy of health records, the right to request a correction to health records, the right to obtain documentation of disclosures of information may be used or disclosed. The current regulation provides protection for paper, oral, and electronic information.
    C. The Confidentiality of Medical information Act, California Civil Code Section 56 et seq.
    D. The Violence Against Women Act, 42 U.S.C. §§13925-14045.
    E. The provisions in California Government Code 11015.5 regarding Personal Information Collected on the Internet. In general, the Government Code ensures that any electronically collected personal information about clients cannot be shared with any third party without the client's written consent.
2. Agency shall only release client records upon prior receipt of a valid written consent, unless otherwise authorized to do so by law.

PRIVACY NOTICES

1. Partner Agencies must adopt an HMIS Privacy Notice and incorporate it into their policies and procedures. In addition, HUD mandates that organizations develop policies and procedures for distributing privacy notices or statements to their employees, which include having employees sign to acknowledge receipt of such notices.

2. A Privacy Notice should be prominently displayed or distributed in the program offices where intake occurs. The Partner Agency should promptly revise and redistribute the Privacy Notice whenever there is a material substantive change to the permitted uses or releases of information, the individual's rights, the Partner Agency's legal duties, or other privacy practices. Partner Agencies should maintain documentation of compliance with the Privacy Notice requirements by retaining copies of the Privacy Notice issued by them. A client has the right to obtain a paper copy of the Privacy Notice from the Partner Agency upon request. If the Agency maintains an agency website, a link to its Privacy Notice must be on the homepage of the Agency's website.

CONTENT OF PRIVACY NOTICE

The Partner Agency must provide a Privacy Notice that explains the reasons for collecting personal information and is written in plain language.

The Partner Agency may use the following language to meet the standards of the privacy notice: "We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law, or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate. You may decline to disclose any information without affecting your ability to access most services, however, some services may require certain information. You will be informed if any information you decline to provide will affect your access to services."

CLIENT CONSENT

1. Partner Agencies must obtain a client's informed written consent using the standard Release of Information form prior to entering information concerning the client into the system. If clients refuse consent their data may be entered into the Marin County HMIS system and not shared with other agencies to allow agencies to meet their HUD reporting requirements. Services should not be denied to the client based on refusal to consent.
2. Client consent is revocable at any time [info on how]
3. Agency shall upload client consent forms to Clarity or shall maintain physical copies of client consent forms and other data entry supporting documentation for a minimum of seven years and shall allow County to conduct annual audits of client records.
4. Agency shall allow clients to view their own HMIS data, upon written request; request changes and corrections in accordance with Agency's procedures; and pursue Agency's grievance process.

CLIENT NOTIFICATION OF DISCLOSURE

Client shall be informed if any of their data is intentionally or unintentionally disclosed within 30 days.

If Partner Agency is unable to contact client after all reasonable efforts are made, including utilizing all contact information and contacting all known contacts, Partner Agency shall create an alert on the client's profile with the details of the disclosure. [Sample disclosure language in appendix]

Willful disclosure may result in termination of HMIS access for the user; inadvertent disclosure may result in additional required training.

CLIENT GRIEVANCE PROCEDURES

If a client has any issue with the HMIS at a particular Partner Agency, the client should work with that agency to resolve the issue. Examples: (could include but not limited to) Disclosure of data, incorrect data not fixed, revoked ROI

If the problem is still not resolved to the client's satisfaction, the client can follow the Partner Agency's grievance procedures or request a Client Grievance Form available on the Marin County HMIS website: [url] Specific instructions for clients, including how to submit a grievance, are listed on the form.

Bitfocus will receive the submitted form and distribute copies to the HMIS Governance Group. The HMIS Governance Group will be notified of all grievances received. Bitfocus will use its reasonable best efforts to investigate the issue and will inform the HMIS Governance Group of the results.

If the issue is not system related, the HMIS Governance Group will recommend the best course of action to handle the grievance.

Any material change(s) resulting from a grievance (system-related or not) will require approval from the HMIS Governance Group.

If a client follows the Partner Agency's grievance procedures for an issue related to HMIS, the Partner Agency shall inform the County's HMIS Lead of the complaint and its resolution.

IV. HMIS SECURITY STANDARDS

The Department of Housing and Urban Development (HUD), in its Proposed Rule for HMIS Requirements [link], requires implementation of specified security standards. These security standards are designed to ensure the confidentiality, integrity, and availability of all HMIS information; protect against any reasonably anticipated threats or hazards; and ensure compliance with all applicable standards by end users.

The Marin County Security Plan includes the following elements: (1) physical safeguards; (2) technical safeguards; (3) user access rules, including rescinding user and/or HMIS Partner Agency access when security violations are suspected. Each portion of this plan is detailed below.

GENERAL RULES

1. Agency staff participating in HMIS shall commit to abide by the governing principles of HMIS and adhere to the terms and conditions of the Agency User Agreement, attached hereto and incorporated herein by reference as Exhibit 1.
2. The Agency shall only request user access to HMIS for those staff that require access to perform their job duties.
3. All users must have their own unique user ID and should never use or allow use of a user ID that is not assigned to them. [See Agency User Agreement].

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

1. Computer Location – A computer used as an HMIS workstation must not be accessible to clients or the public. The HMIS workstation must be secured whenever staff are not present to ensure that HMIS data are secure and not accessible by unauthorized individuals.
2. Printer location – Documents printed from HMIS must be sent to a printer in a secure location where only authorized persons have access.
3. Line of Sight – Non-authorized persons should not be able to see an HMIS workstation screen. Monitors should be turned away from the public or clients in order to protect client privacy.

TECHNICAL SAFEGUARDS

WORKSTATION SECURITY

1. The HMIS Lead Agency will enlist the use of PKI (Public Key Infrastructure) or another suitably secure method to identify approved workstations, in compliance with Public Access baseline requirement in the HUD Data Standards. The Partner Agency Security Officer will verify that a current PKI certificate (available from the HMIS System Administrator) has been installed on each End User's workstation.
2. Partner Agency 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).
3. Partner Agency will confirm that any workstation accessing HMIS has and uses a firewall.

ESTABLISHING HMIS USER IDS AND ACCESS LEVELS

1. The HMIS Partner Agency Technical Administrator will ensure that any prospective End User reads, understands and signs the HMIS End User Agreement.
2. The HMIS Partner Agency Technical Administrator is responsible for ensuring that all agency End Users have completed mandatory trainings prior to being provided with a User ID to access HMIS.
3. All End Users will be issued a unique User ID and password by Bitfocus. Sharing of User IDs and passwords by or among more than one End User is expressly prohibited. Each 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.
4. The HMIS Partner Agency Technical Agency Administrator will always attempt to approve the most restrictive access that allows the End User to efficiently and effectively perform his/her assigned duties.
5. The HMIS Partner Agency Technical Administrator will notify Bitfocus when new users are approved for usernames and passwords.
6. The HMIS Partner Agency Technical Administrator will notify Bitfocus which access level to assign to each authorized user. Access levels may vary across HMIS Partner Agencies, depending upon their involvement with coordinated entry, contract monitoring, program and system evaluation, and other factors.
7. When the HMIS Partner Agency Technical Administrator determines that it is necessary to change a user's access level, the Partner Agency HMIS Partner Agency Technical Administrator will notify Bitfocus as soon as possible.

OTHER TECHNICAL SAFEGUARDS

1. The HMIS Partner Agency shall develop and implement procedures that will prevent unauthorized users from connecting to private agency networks, whether or not they are used to access HMIS.
2. Unencrypted PPI may not be transmitted in any fashion, including sending file attachments by unencrypted email. All downloaded files containing PPI must be deleted from the workstation temporary files and the "Recycling Bin" emptied before the End User leaves the workstation.
3. Encrypted hard drives are recommended

PASSWORDS

1. All 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.
2. 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 numbers, lowercase letters, capital letters; and/or special characters (e.g. ~ ! @ # $ % ^ & * ( ) _).
3. End users may be prompted by the software to change their password from time to time.
4. End Users must immediately notify their HMIS Partner Agency Technical Administrator and/or Security Officer if they have reason to believe that someone else has gained access to their password.
5. Three consecutive unsuccessful attempts to login will disable the User ID until the password is reset. All user passwords will be reset by Bitfocus.

USER ACCESS

REQUEST NEW USER ID

1. When the Agency Administrator identifies a staff member that requires access to HMIS, Agency Administrator shall have the prospective user complete online Clarity HMIS training provided by Bitfocus and shall inform Bitfocus of the need to create the new user.
2. Bitfocus shall create a new user ID and notify the user ID owner of how to create a password via email.

CHANGE USER ACCESS

1. When the Agency Administrator determines that it is necessary to change a user's access level, the Agency Administrator will inform Bitfocus of the update to be made.

RESCIND USER ACCESS

1. When a HMIS Agency user leaves Agency or no longer requires HMIS access, Agency Administrator shall Contact HMIS support to remove their name from the user list within 24 hours.
2. Bitfocus reserves the right to terminate End User licenses that are inactive for 90 days or more. The HMIS System Administrator will attempt to contact the HMIS Partner Agency Technical Administrator for the End User in question prior to termination of the inactive user license.
3. In the event of suspected or demonstrated noncompliance by an End User with the HMIS End User Agreement or any other HMIS plans, forms, standards, policies, or governance documents, Bitfocus will

deactivate the User ID for the End User in question until an internal agency investigation has been completed. The HMIS Partner Agency Technical Administrator will notify Bitfocus 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.

4. In the event the HMIS Partner Agency Technical Administrator is unable or unwilling to conduct an internal investigation as described above, Bitfocus is empowered to deactivate any user IDs pending its own investigation of an End User's suspected noncompliance with the HMIS End User Agreement, or any other HMIS plans, forms, standards, policies, or governance documents.
5. Marin County is empowered to permanently revoke a Partner Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the Marin County HMIS Policies & Procedures, or the Partner Agency MOU.

RESET PASSWORD

1. When a HMIS Agency user forgets his or her password or has reason to believe that someone else has gained access to their password, they must immediately notify Bitfocus.
2. Bitfocus will reset the user's password and notify the user of the new temporary password.

V. HMIS DATA

OVERVIEW

1. HMIS Data is highly confidential. Agency agrees that it shall not use or disclose information other than as permitted or required by this agreement or as required by law.
2. Agency shall use appropriate standards to prevent use or disclosure of the information other than as permitted by this agreement. Agency owns and is responsible for the client data associated with its own programs. Agency is encouraged to use its own HMIS data for public relations, reporting and funding as long as client confidentiality is maintained.
3. While acting within this agreement, Agency has the ability to view information for its own programs, enter and edit information, enter unlimited numbers of clients and services, run unlimited numbers of reports, and to export data for further reporting.
4. As set forth in Section 1. the County will publish quarterly community-wide aggregate HMIS homeless data (not agency specific). These reports will be raw point-in-time data. Agency may also use published HMIS data.
5. The County will not release proprietary information about agencies, their services, procedures, or client demographics without permission of the agency.
6. The County may use HMIS data for planning, reporting and grant writing processes including Consolidated Plans, Gaps Analysis, HUD reporting, Emergency Solutions Grants, etc., and may reconcile and release aggregate data.

COLLECTION AND ENTRY OF CLIENT DATA

1. As a contributing HMIS Agency, Agency shall enter client specific data into HMIS that is accurate, complete, and timely and in accordance with the following requirements:
    a. Agency shall gather client data according to the policies, procedures and confidentiality rules of the Agency.

b. Agency shall collect all universal and applicable program data elements from the most current version of the HUD HMIS Data and Technical Standards.
c. Agency shall keep all client data entered into HMIS as accurate and as current as possible.
d. Agency shall continue to maintain hardcopy or electronic files according to Agency's requirements.
e. Any authorized data imports will be the responsibility of Agency.
f. Agency is responsible for the accuracy, integrity, and security of all data input by Agency.
g. Agency is responsible for a baseline of data quality to include: non-duplication of client record, Universal & Program level data elements as defined by HUD Data Standards, up-to-date Program Entries and Exits.

HMIS DATA QUALITY

Data quality shall be a concern of highest importance to the Agency, which will use its best efforts to continuously improve quality. Quality assurance shall be the ultimate responsibility of Agencies, in consultation with County as the HMIS Lead Agency.

DATA TIMELINESS

HUD Universal and Program-Specific data elements should be entered within 3 business days of intake, annual assessment, and exit.

DATA QUALITY IMPROVEMENT PLAN

Bitfocus will send periodic reports on data quality and completeness to Partner Agencies. Partner Agencies shall correct missing or incorrect data to the best of their ability in a timely fashion to allow Bitfocus to complete HUD and state reporting.

As needed, Partner Agencies and HMIS Lead Agency will collaborate on a data quality improvement plan.

VI. CUSTODY OF DATA

1. The Agency acknowledges, and the County agrees, that the Agency retains ownership over all information it enters into the Marin County HMIS system.
2. In the event that the HMIS ceases to exist, Agency will be notified by the County and provided reasonable time to access and save client data on those served by the Agency, as well as statistical and frequency data from the entire system. Thereafter, the information collected by the centralized server will be purged or appropriately stored by the County.
3. In the event that the County ceases to be the Lead HMIS Agency, County will use its best efforts to transfer the custodianship of the data within Marin County HMIS to another organization for continuing administration, and Agency will be informed in a timely manner.
1.

Homeless Management Information System
Client Grievance Instructions

HMIS Clients are encouraged to work with the agency they are having issues with before submitting a grievance. A grievance should be used as a last resort. All grievances are taken VERY seriously, and reviewed by the Marin HMIS Committee on an individual basis. If you have not been able to resolve your issue with the agency directly, please complete the attached form.

- Complete ALL fields
- Print Legibly
- Be as specific and as detailed as possible
- Attach additional pages as necessary
- Sign and Date the form

After you have completed the form, please email the form to [email] or deliver the form to Bitfocus, Inc. via US Mail at:

Bitfocus, Inc.
5940 S Rainbow Blvd Ste 400, #60866
Las Vegas, Nevada 89118-2507

Homeless Management Information System (HMIS)
Client Grievance Form

_____

Client Name

_____

Agency Name – List the agency you have been working with to solve this issue

_____

Agency Contact Person – List the name and phone number of the person you have been working with to solve this issue

_____

First date of problem – List the date you first began working on this issue.

Description of issue. Please use the space below to describe your issue. Please print legibly and be as detailed as possible. Attach additional pages as needed. Issue must relate to HMIS, such as [examples]. For other grievances, please see the agency's grievance policy.

Please sign and date below:

_____ _____

Client Signature Date