Table of Contents

Santa Clara County HMIS
Standard Operating Procedures

Section 1: Contractual Requirements and Roles

Bitfocus, Inc. Contractual Requirements: Bitfocus, Inc. ("Bitfocus"), in its role as Santa Clara County Homelessness Management Information System ("SCC HMIS") Software as a Service ("SaaS") vendor, will use its reasonable best efforts to provide all of the necessary equipment and staff to configure, operate, and maintain the HMIS database. In addition, Bitfocus will use its reasonable best efforts to provide technical assistance as it pertains to software and relevant hardware. In its role as SCC HMIS System Administrator, Bitfocus will use its reasonable best efforts: to facilitate and coordinate all activities in the operation and implementation of the HMIS, including assisting all participating housing and services providers (the "Partner Agencies") to meet relevant HUD requirements; to provide end-user training, data quality assessment, help desk support, and other technical support; and to provide decision support. Additional services may be provided on a case-by-case basis, as agreed upon by Bitfocus, a Partner Agency, and the County of Santa Clara's Office of Supportive Housing ("County"), the Santa Clara County Continuum of Care's ("CoC") HMIS Lead.

Contractual Requirements for Database: Security of equipment and data is a priority for Bitfocus. These Standard Operating Procedures ("SOPs") outline the foundation for system security including the usage policy for access to the database, standards for data exports and imports for data analysis purposes, as well as the procedures for maintaining the database and data integrity.

SCC CoC Board: The Santa Clara County CoC Board ("CoC Board") governs the HMIS project. The CoC Board is representative of CoC organizations and of projects serving homeless subpopulations, includes at least one homeless or formerly homeless individual, and includes representatives of public and private organizations in Santa Clara County. These include consumers, agencies funded by the U.S. Department of Housing and Urban Development ("HUD"), homeless services providers, local governments, and state government. The procedures used to select members for the CoC Board can be found in the CoC Governance Charter found on the Santa Clara County Office of Supportive Housing website.

Database Management Roles: Management of an HMIS requires several skill sets. These duties will be performed by a System Administration team comprised of CoC Board identified roles to provide the best and most efficient service to SCC HMIS stakeholders:

- SCC HMIS System Administrator—assigns rights for users; merges duplicate files; manages maintenance reporting, backups, and security; updates policy and procedures; monitors login attempts; completes system updates; approves any changes to the system; conducts maintenance and disaster planning; going

onsite if necessary to resolve questions about the software or training; and supervises personnel.

- Systems Analysts and Help Desk Support—assists in the design of reports as needed by Partner Agencies and community stakeholders; answers user questions; and assists users in resolving problems.

As the user base grows, it is understood that these positions and roles will be re-evaluated to meet the needs of stakeholders.

New Agency Contractual Requirements and Roles: Any agency wishing to participate in the SCC HMIS must execute a Partner Agency Privacy and Data Sharing Agreement (MOU).

The roles of every Partner Agency are defined in order to prevent confusion regarding responsibilities and privileges. The following roles must be filled in order for an agency to begin using HMIS:

- ❑ Partner Agency Technical Administrator
- ❑ Partner Agency Security Officer
- ❑ Partner Agency End User

Note: In some cases, more than one role will be assigned to the same individual.

The *Partner Agency Technical Administrator* is able to edit, create, and append data for all programs and services operated by his or her agency; and is able to run reports regarding agency programs and services. Additional rights and responsibilities are outlined in the Santa Clara County HMIS Partner Agency Technical Administrator and Security Officer Agreement.

The *Partner Agency Security Officer* will conduct quarterly compliance reviews; ensure that all End Users at their agency sign and execute applicable Santa Clara County HMIS End User Agreements; and ensures that all End Users at their agency complete required trainings. Additional rights and responsibilities are outlined in the Santa Clara County HMIS Partner Agency Technical Administrator and Security Officer Agreement. A quarterly compliance checklist is attached as Appendix B.

The *Partner Agency End User* is able to create client files and run reports against the data collected at their agency; able to update and append client records; and able to view sensitive portions of the record if the client has consented and signed a release.

The *Continuum of Care Data Analyst* is able to view global reports regarding homeless persons in our community, demographics, service utilization, total statistics and numbers regarding persons in the system.

The *Continuum of Care Representative* is able to view aggregate-level reports, demographics, service utilization, total statistics and numbers regarding data in the system.

The *Continuum of Care Program Manager* is able to view program-level data at any agency they are responsible for monitoring.

All users of the system should recognize that rights are assigned on a need-to-know basis.

Section 2: Participation Requirements

Participation Policy: Agencies that are funded as part of the Santa Clara County Continuum of Care to provide homeless programs and/or services will be required to participate in the HMIS, with the exception of Victim Service Providers, who are required to utilize a comparable database[1]. All other homeless providers are strongly encouraged to participate in the HMIS.

Participation Requirements: For most efficient utilization of the services provided by the SCC HMIS, several steps must be completed at the agency level before implementation can begin. Although the System Administrator can assist with most steps, agencies should be prepared to act without assistance. These steps include:

- Acquisition of High Speed Internet Connectivity with at least one static IP address;
- Identification of an on-site Technical Administrator to serve as the primary contact, or the name of an outside contractor;
- Identification of a Security Officer;
- Completion of a network and security assessment to comply with the U.S. Department of Housing and Urban Development's (HUD's) HMIS Rule, and/or HUD's HMIS Data Standards, and/or HUD's Continuum of Care Program Rule, as applicable;
- Signing and executing a Partner Agency Privacy and Data Sharing Agreement (MOU) or other applicable agreement(s); and
- Adopting written procedures concerning client consent for release of information, client grievance procedures, and interview protocols as specified in this document.

Implementation Requirements: Partner Agencies must generate or obtain documents that cover each of the following areas in order for implementation to begin.

[1] HUD defines a victim service provider to mean a private nonprofit organization whose primary mission is to provide direct services to victims of domestic violence. This term includes permanent housing providers—including rapid re-housing, domestic violence programs (shelters and non-residential), domestic violence transitional housing programs, dual domestic violence and sexual assault programs, and related advocacy and supportive services programs. https://www.hudexchange.info/faqs/2686/how-does-hud-define-victim-service-provider/

Written Client Consent for Data Entry:

Partner Agencies must obtain a client's informed written consent prior to entering information concerning the client into the system. If a client does not consent, services should not be denied to the client. The agency can use the client consent refused protocol in appropriate cases. Partner Agencies must use the forms approved by the CoC Board. Partner Agencies that share protected health information must have internal procedures for obtaining a client's informed written consent prior to the sharing of this information.

Privacy Statement: Partner Agencies must adopt an HMIS Privacy Statement 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. The Privacy Statement is discussed in further detail in Section 12 of these SOPs. A sample Statement is attached as Appendix C.

Interview Protocols: Each Partner Agency must develop a written program-specific interview guide that includes the minimal data elements and any additional elements the Partner Agency wishes to collect.

Background Check Procedures: Each Partner Agency is responsible for conducting its standard employment background check for any employee, contractor, or volunteer who will use the HMIS.

Staff Confidentiality Agreements: Each Partner Agency must develop a procedure for informing staff of client confidentiality. All users of the system must complete the Clarity Human Services General Training prior to being authorized to use the system. In addition, all users of the system are required to complete the Santa Clara County Client Consent Training annually.

Information Security Protocols: Internal policies must be developed at each Partner Agency to establish a process for the detection and prevention of a violation of any HMIS information security protocols.

Virus Prevention, Detection, and Disinfection Protocols: Participation in the HMIS requires that Partner Agencies develop procedures intended to assure that computers with access to the HMIS run updated anti-virus software.

Data Collection Commitment: Participation in the HMIS requires that all Partner Agencies collect minimum data elements on all consenting clients in accordance with HUD requirements, unless the County has granted an exception.

Connectivity: Once implementation has begun, each Partner Agency agrees to use its reasonable best efforts to maintain appropriate Internet connectivity in order to continue participation.

Maintenance of Onsite Computer Equipment: Each Partner Agency agrees to use its reasonable best efforts to maintain computer equipment to the extent required to continue participation.

Conversion of Legacy Data or Links to Other Systems: Partner Agencies using other systems or desiring to have legacy data converted must provide resources and processes that enable conversion without cost to Bitfocus or the County.

Section 3: Training

Clarity General and SCC HMIS Client Consent Training: Bitfocus will provide training to instruct all HMIS users in the proper procedures to operate the HMIS. Bitfocus will also provide training about each user's responsibility to protect client privacy and ensure that basic system security is maintained, such as logging out of HMIS when it is not in use

Partner Agency Technical Administrator and Security Officer Training: Each Partner Agency will have a Technical Administrator and Security Officer. Each Partner Agency will have a representative participate in any training offered specifically for Technical Administrators and/or Security Officers. Such training will take place in Santa Clara County or by webinar. When offered, these trainings will cover practical problem solving strategies needed to improve the operation or security of the HMIS.

End User Training Schedule: Bitfocus will provide regular training in the day-to-day use of the HMIS and will announce training dates in advance. The following trainings are available on demand:

- Data Standards for End Users
- General HMIS Requirements
- Santa Clara County Entry/Exit Shelter Workflow Training
- Santa Clara County Coordinated Entry Updates
- Santa Clara County Client Consent Training
- Clarity Human Services: Frequently Asked Questions- System Administration Communities
- Clarity Human Service: General Training

Additional in person or web-based workflow trainings are developed upon request and in coordination with the appropriate Program Manager from the County.

Training will use an established demo database, and it will cover the following topics: intake, assessment, information and referral, reports, privacy, and client tracking. Training requires a three to four-hour commitment. Training on any agency-modified fields or screens will be the responsibility of the Partner Agency making the modification.

Section 4: User, Location, Physical and Data Access

Access Privileges to the SCC HMIS: Access to system resources will only be granted to Partner Agency staff that need access in order to perform their duties.

Access Levels for SCC HMIS Users: Each user of the system will be assigned an account that grants access to the specific system resources that he or she requires. A model of least-privilege is used; no user will be granted more than the least amount of privilege needed to perform his or her duties.

Access to Data: All data collected by the SCC HMIS will be categorized. Access to data sets, types of data, and all other information housed as part of the SCC HMIS is governed by policies approved by the CoC Board and Bitfocus. Reproduction, distribution, destruction of, and access to the data are based on the content of the data. At no time may identifying confidential data be distributed or accessible without the consent of the client(s) in question.

Access to Client Paper Records: Partner Agency users should not have greater access to client information through the SCC HMIS than is available through the agency's paper files.

Physical Access Control: The building containing the central server is secured through locked key access. The room housing the central server has keyed entry with access to keys limited to Bitfocus, Inc. staff only.

System access over wireless networks: Access to the HMIS over any type of public wireless network is discouraged. Public wireless networks are more susceptible to unauthorized access than private wireless networks. For private networks, only Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access II (WPA2) security protocols are allowed.

Unique User ID and Password: Each user of the system must be individually and uniquely identified. Identification will be verified through a password. Users are not permitted to share their password or permit other users to log in to the system with their password. Passwords will be at least eight characters long and meet reasonable industry standard requirements. These requirements are:

1) Using a combination of at least 3 of the following:
    a. Numbers;
    b. Lowercase letters;
    c. Capital letters; and
    d. Special characters (e.g. ~ ! @ # $ % ^ & * ( ) _);

2) Not using, or including, the username, the SCC HMIS name, or the SCC HMIS vendor's name; and
3) Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

Written information specifically pertaining to user access (i.e., username and password) may not be stored or displayed in any publicly accessible location. Individual users will not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time.

Right to Deny User and Partner Agencies' Access: The HMIS Lead Agency and Bitfocus have the right to suspend, limit, or revoke the access of any Partner Agency or individual for violation of SCC HMIS policies, including these SOPs. Upon remedy of a proven violation and completion of additional training (as needed), access rights may be reinstated. If privileges have not been reinstated, the Partner Agency or individual may file an appeal to the CoC Board for reinstatement.

Monitoring: Access to the SCC HMIS will be monitored. In addition, the SCC HMIS will maintain logs of all actions taken within the system, including login transactions and detailed monitoring of user data transactions within the software. Bitfocus will use its reasonable best efforts to review logs on a regular basis. It is understood that Partner Agencies will cooperate with all monitoring requirements. All exceptions that show security policy violations will be investigated.

Data Integrity Controls: Access to the production data is restricted to essential system administrative staff only. Each staff member that has access to production data is contracted not to alter or impact the data in any adverse way.

Section 5: Technical Support and System Availability

Planned Technical Support: Bitfocus will use its reasonable best efforts to offer technical support to all Partner Agencies. Support services of the SCC HMIS include: training, implementation support, report writing support, and process troubleshooting.

Partner Agency Service Requests: System administrative staff is only permitted to respond to service requests that are submitted in writing by the Partner Agency Technical Administrator or Security Officer.

Partner Agency Technical Support: Partner agency staff may reach Bitfocus Technical Support for general user inquiries.

Rapid Response Technical Support: An emergency contact number will be provided for requests for service that require a rapid response (i.e., unable to access system). These service requests will be prioritized above other requests. Partner Agencies should plan accordingly.

Availability: The goal is to have the system available 24 hours a day, subject to scheduled outages for updating and maintenance. Bitfocus will use its reasonable best efforts to achieve a 99% uptime. On occasion, there will be planned system outages. Partner Agencies will be notified a minimum of 48 hours before a planned but unscheduled outage is to occur. Bitfocus will use its reasonable best efforts to address unplanned interruptions within 24 hours, and agencies will be notified when the system becomes available.

Section 6: Stages of Implementation

Stage 1 – Purpose: Partner Agencies must identify the program(s) that provide services to households experiencing homelessness, households at eminent risk of homelessness, or formerly homeless households.

Stage 2 – Startup: Partner Agencies must complete all MOUs and agreements, and adopt all policies and procedures required in these SOPs.

Stage 3 – Organization Data Entry: Partner Agencies must define the organization and provide detailed descriptions of programs and eligibility, as well as define user workflow.

Stage 4 – Initial System Rollout: Partner Agencies must ensure that Clarity General and SCC HMIS Client Consent trainings are completed by Technical Administrators, Security Officers, and End Users. They must also define users and responsibilities. All HMIS training will be conducted using a demonstration version of the software and data. Real client data will **NEVER** be used for training purposes.

Stage 5 – Client Data Entry: Partner Agencies must begin entering client information into the SCC HMIS.

Stage 6 – Client-Program Entry: Partner Agencies must begin entering client enrollment into their programs.

Stage 7 – Case Management: Partner Agencies may use the SCC HMIS as a case management tool in the day-to-day operation of the agencies if such agencies wish to do so.

Stage 8 – Program Management: Partner Agencies may use the SCC HMIS to track program performance on an agency level.

Section 7: Encryption Management

Encryption General: All information should be encrypted in the database per HUD standards. All connections to the SCC HMIS should be encrypted to HUD standards or higher. Encryption

should be sufficient to prevent unauthorized personnel from accessing confidential information for any reason.

Encryption Management: In the event that system-wide data decryption becomes necessary, the CoC Board must obtain the written authorization of every Partner Agency's Executive Director.

Section 8: Data Release Protocols

Sharing Protected Information: A Client Consent for Data Collection and Release of Information (ROI) document indicating what information the client agrees to have shared with other partner agencies must be signed prior to sharing of any Protected Personal Information ("PPI") including identifying information (such as the client's name, birth date, gender, race, social security number, phone number, residence address, photographic likeness, and other similar identifying information) and financial information (such as the client's employment status, income verification, public assistance payments or allowances, food stamp allotments, and other similar financial information).

The Client Consent for Data Collection and Release of Information (ROI) form will be a dated document with a defined term. Before any data will be entered into the SCC HMIS, the client must first consent to data entry and agree to what information can be entered. Upon completion of the approved consent form, the Partner Agency will create a profile for the client. The SCC HMIS will assign the client a unique personal identifier. The Partner Agency will upload the ROI into the SCC HMIS, and only enter the information into the system that has been approved by the client. Partner Agencies will only be able to access the information specified on the form that was entered into the system during the time the form was in effect. Partner Agencies should also note that services must not be contingent on a client consenting to data entry.

The client can revoke his or her consent at any time, in full or in part, and have his or her file deactivated, by submitting a written and signed request to revoke their consent. In emergency situations, such as domestic violence, clients may revoke consent verbally to Partner Agency staff.

Anonymous Client Data Entry: In the event that a client does not want to have personally identifying information entered into the HMIS, he or she will be entered following the Anonymous Client Data Entry Protocol listed below.

Basic Consent Refused Client Record Data Entry Protocol

1. Start with Quality of Name field and enter "Partial, street name, or code name reported"
2. Enter zeros for SSN
3. Change to "Client Doesn't Know" for Quality of SSN
4. Type "Refused" for Last Name

5. Type “Ooooo” (letter “o” not zero) for First Name
6. Enter 01/01/ and approximate year of birth
7. Enter “Approximate or partial DOB reported” for Quality of DOB
8. Enter Gender, Race, Ethnicity and perhaps Veteran status with real data if it won’t serve to identify them in any way
9. Leave Middle Name and Suffix blank
10. Click Add Record
11. In the “Unique Identifier” field that now appears with an auto-filled number, copy and paste that into the Last Name field, eliminating the word “Refused”. If you don’t do this, you won’t have an identifier in the top of each screen as you continue to enter data on this client.

Printed Information: Printed records disclosed to the client or another party should indicate the identity of the individual or agency to whom the record is directed, the date, and the initials of the person making the disclosure.

Requests for SCC HMIS Client Information: The Partner Agency must notify the SCC HMIS System Administrator within one working day when the Partner Agency receives a request from any individual or outside agency for client-identifying information.

Case Notes: It is understood that client case notes will not be shared, and that each Partner Agency will have the ability to enter its own private notes about a client.

Continuum Approved Uses and Disclosures: HMIS client data may be used or disclosed for case management, administrative, billing, and analytical purposes, or other purposes as required by law. “Uses” involve sharing parts of client information with persons within an HMIS Partner Agency. “Disclosures” involve sharing parts of client information with persons or organizations outside of an HMIS Partner Agency.

Data Release Criteria: No identifiable client data will be released to any person, agency, or organization that is not the owner of said data for any purpose other than those specified in the *Santa Clara County HMIS Client Consent for Data Collection and Release of Information* without written permission from the individual in question.

Aggregate Data Release Criteria:
All data must be anonymous, either by removal of all identifiers and/or all information that could be used to infer an individual or household’s identity. Identifiers include, but are not necessarily limited to: (1) name; (2) Social Security number; (3) date of birth. The CoC Board must approve releases of anonymous client-level data for research purposes. Aggregate data must meet appropriate data quality and coverage standards.

Anonymous Client-level Data Release Criteria:

All data must be anonymous, either by removal of all identifiers and/or all information that could be used to infer an individual or household's identity. Identifiers include, but are not necessarily limited to: (1) name; (2) Social Security number; (3) date of birth.

Section 9: HMIS Security Plan

The Department of Housing and Urban Development (HUD), in its Proposed Rule for HMIS Requirements, 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 Santa Clara County Security Plan includes the following elements: (1) designated security officers; (2) quarterly and annual security audits; (3) physical safeguards; (4) technical safeguards; (5) rescinding user and/or HMIS Partner Agency when security violations are suspected.

Each portion of this plan is detailed below.

Security Officers

The HMIS Lead Agency and all HMIS Partner Agencies must designate Security Officers to oversee HMIS privacy and security.

<u>Santa Clara County Lead Security Officer</u>

1. Bitfocus, Inc., in its role as HMIS System Administrator, is the Lead Security Officer.
2. Bitfocus will assess security measures in place prior to establishing access to HMIS for any new Partner Agency.
3. Bitfocus will review and maintain files of Partner Agency annual compliance certification checklists.
4. Bitfocus will conduct regular security audits of Partner Agencies.

<u>Partner Agency Security Officer:</u>

1. May be the HMIS Partner Agency Technical Administrator or another Partner Agency employee, volunteer or contractor who has completed the Clarity General and SCC HMIS Client Consent trainings and is adequately skilled to assess HMIS security compliance
2. Conducts a security audit for any workstation that will be used for HMIS data collection or entry
   a. no less than quarterly for all agency HMIS workstations, AND
   b. prior to issuing a User ID to a new HMIS End User, AND
   c. any time an existing user moves to a new workstation.
3. Continually ensures each workstation within the Partner Agency used for HMIS data collection or entry is adequately protected by a firewall and antivirus software (per Technical Safeguards – Workstation Security)

4. Completes the Quarterly Compliance Certification Checklist, and forwards the Checklist to the Lead Security Officer.

Security Audits

New HMIS Partner Agency Site Security Assessment

Prior to establishing access to HMIS for any new Partner Agency, the Lead Security Officer will assess the security measures in place at the Partner Agency to protect client data. The Lead Security Officer will meet with the Partner Agency Executive Director (or executive-level designee), HMIS Partner Agency Technical Administrator and Partner Agency Security Officer to review the Partner Agency's information security protocols prior to recommending that Santa Clara County countersign the HMIS MOU. This security review shall in no way reduce the Partner Agency's responsibility for information security, which is the full and complete responsibility of the Partner Agency, its Executive Director, and its HMIS Partner Agency Technical Administrator/Security Officer.

Quarterly Partner Agency Self-Audits

1. The Partner Agency Security Officer will use the HMIS Quarterly Compliance Certification Checklist to conduct quarterly security audits of all Partner Agency HMIS End User workstations.
2. If areas are identified that require action due to noncompliance with these SOPs, the Partner Agency Security Officer will note these on the Compliance Certification Checklist, and the Partner Agency Security Officer and/or HMIS Agency Technical Administrator will work to resolve the action item(s) within 15 days.
3. Any Compliance Certification Checklist that includes one or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved. The Checklist findings, action items, and resolution summary must be reviewed and signed by the Partner Agency Executive Director or other empowered officer prior to being forwarded to the Lead Security Officer.
4. The Partner Agency Security Officer must turn in a copy of the Compliance Certification Checklist to the Lead Security Officer on a quarterly basis.

Annual Security Audits

1. The Lead Security Officer will schedule annual security audits in advance with selected Partner Agency Security Officers.
2. The Lead Security Officer will use the Quarterly Compliance Certification Checklist to conduct security audits.
3. The Lead Security Officer will randomly audit at least 10% of the workstations for each HMIS Partner Agency selected for review. In the event that an agency has more than 1 project site, at least 1 workstation per project site will be audited.
4. If areas are identified that require action due to noncompliance with these standards or any element of these SOPs, the Lead Security Officer will note these on the Compliance Certification Checklist, and the Partner Agency Security Officer and/or HMIS Partner Agency Technical Administrator will work to resolve the action item(s) within 15 days.

5. Any Compliance Certification Checklist that includes one or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved and the Checklist findings, action items, and resolution summary has been reviewed and signed by the Partner Agency Executive Director or other empowered officer and forwarded to the HMIS Lead 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 SCC HMIS Client Consent training within the past 12 months

1. Computer Location – A computer used as an HMIS workstation must be in a secure location where only authorized persons have access. The HMIS workstation must not be accessible to clients or the public. HMIS-trained and non-HMIS trained staff may use the same computers.
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. To promote the security of HMIS and the confidentiality of the data contained therein, access to HMIS will be available only through approved workstations.
2. Partner 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).
3. Two-Factor Authentication (2FA) is enabled to confirm the user's identity.
4. Partner Agency Security Officer will confirm that any workstation accessing HMIS has and uses hardware or software firewalls.

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 and maintain a file of all signed HMIS End User Agreements.
2. The HMIS Partner Agency Technical Administrator is responsible for ensuring that all agency End Users have completed mandatory trainings, including the Clarity General SCC HMIS Client Consent trainings prior to being provided with a User ID to access HMIS. VI-SPDAT or HPAT training is required to edit or create client assessments in the SCC HMIS. If the VI-SPDAT or HPAT training is not completed the user access will be limited. If the user later completes this training access to assessments will be reinstated.
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 Security Officer 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 stored or transmitted in any fashion—including sending file attachments by email or downloading reports including PPI to a flash drive, to the End User's desktop, or to an agency shared drive. 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.

<u>Rescinding User Access</u>

1. End User access should be terminated within 24 hours if an End User no longer requires HMIS access to perform his or her assigned duties due to a change of job function or

termination of employment. The HMIS Partner Agency Technical Administrator is responsible for notifying Bitfocus so that access can be terminated within the specified timeframe.

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 or Security Officer 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.

Santa Clara County is empowered to permanently revoke a Partner Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the Santa Clara County HMIS Standard Operating Procedures, or the Partner Agency MOU.

Section 10: Internal Operating Procedures

Computer Virus Prevention, Detection, and Disinfection: The goal of the SCC HMIS will be to incorporate and maintain updated virus protection from a reputable single source. Any and all viruses found will be quarantined and analyzed. If irreparable, the virus will be deleted. Partner agencies are required to run and maintain their own antivirus software from an approved source on all computers that have access to the SCC HMIS system.

Operating System Updates: The goal will be to update or patch the SCC HMIS within a reasonable time after review of the vendor's release of updates and patches and approval by the system administrator.

Backup and Recovery: The goal will be to back up the SCC HMIS on a daily basis. Backups will be stored electronically offsite. A backup of hardware and SCC HMIS software will be stored in an offsite location so that it will be available in the event of a catastrophic failure.

Disaster Recovery Process: The goal will be to review disaster recovery processes and check offsite systems for viability twice per year.

Community Reporting Process: At the direction of the County, Bitfocus will publish community-wide aggregate reports or dashboards summarizing information about the clients in the HMIS on a periodic basis. The County and Bitfocus will ensure that all published reports or dashboards do not include any personally identifying information or links to PII.

Termination of the HMIS system: In the event the SCC HMIS terminates, Partner Agencies will be notified and provided a reasonable period of time to access and save client data as well as statistical and frequency data from the entire system. Then, the information on the database will be purged or stored. If the latter occurs, the data will remain in an encrypted and aggregate state.

Termination of Bitfocus as Program Administrator: In the event Bitfocus is terminated as the System Administrator, custodianship of the data on the SCC HMIS will be transferred to the County or to a successor System Administrator, and all Partner Agencies will be informed in a timely manner.

Section 11: SCC HMIS Client Grievance Procedures

If a client has any issue with the SCC HMIS at a particular Partner Agency, the client should work with that agency to resolve the issue.

If the problem is still not resolved to the client's satisfaction, the client can follow the Partner Agency's grievance procedures or request an SCC HMIS Grievance form available on the Santa Clara County HMIS website: scc.hmis.cc. A copy of the form is included in Appendix D. Specific instructions are listed on the form.

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

If the issue is not system related, the County 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 CoC Board.

Section 12: SCC HMIS Privacy Statement

An individual has a right to adequate notice of a Partner Agency's use and release of PPI and of the individual's rights, as well as the Partner Agency's legal duties, with respect to PPI. A Privacy Statement should be prominently displayed or distributed in the program offices where intake occurs. The Partner Agency should promptly revise and redistribute the Privacy Statement 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 Statement requirements by retaining copies of the Privacy Statements issued by them. A client has the right to obtain a paper copy of the Privacy Statement from the Partner Agency upon request.

Content of Privacy Statement: The Partner Agency must provide a Privacy Statement that is written in plain language and contains the elements required by this section. These elements are not exclusive, and either oral or written notice may inform the individual of the permitted uses and releases of information. The following, or a substantially similar, statement must be prominently displayed: ''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.''

- A description of each of the purposes for which a Partner Agency is permitted or required by this notice to use or release PPI without the individual's written consent or authorization. These include administrative, programmatic, and academic research purposes.

- If a use or release of information is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the more stringent law.

- A statement that consensual uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization.

- A statement of the individual's rights with respect to PPI and a brief description of how the individual may exercise these rights.

- A statement that the Partner Agency is required by law to maintain the privacy of PPI and to provide individuals with notice of its legal duties and privacy practices with respect to protected personal information.

- A statement that the Partner Agency is required to comply with the terms of the notice currently in effect.

- A statement that reserves the right to change the terms of the notice and to make the new notice provisions effective for all PPI. The statement must also describe how the Partner Agency will attempt to provide individuals with a revised notice.

- A statement that individuals may complain to the Partner Agency if they believe their privacy rights have been violated.

- A brief description of how the individual may file a complaint with the Partner Agency.

- A statement that the individual will not be retaliated against for filing a complaint.

- The name, or title, and telephone number of a person or office to contact for further information.

- The date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published

Section 13: Participation without using Clarity Human Services software (data integration)

The Santa Clara County CoC does not permit data integration.

Section 14: User Meetings

User meetings will be scheduled periodically with advance notice given via the SCC HMIS mailing list and posted on the Santa Clara County HMIS website: scc.hmis.cc The Bitfocus staff responsible for SCC HMIS matters should be available to confer with partner agencies via phone, e-mail, or in person.

While most meetings will be optional to attend, it may be necessary to request mandatory attendance at a particular meeting. If this becomes necessary, ample notice will be given.

Section 15: Guidelines on Removing Partner Agencies or Users

Voluntary Removal: If a Partner Agency or user no longer wants to access the SCC HMIS, they simply need to inform Bitfocus of such decision. In the case of user removal, it is the Partner Agency's responsibility to contact Bitfocus in a timely manner so the User ID can be deactivated to prevent unauthorized access to the system. A Partner Agency requesting removal from the SCC HMIS understands the following:

1) The Partner Agency will receive one copy of the data it has input into the SCC HMIS. Such copy will be in a format determined by Bitfocus and approved by the County. The Partner Agency will be given an appropriate description of the data format.
2) The data the Partner Agency enters into the system will remain in the system for the purposes of producing aggregate non-identifying reports. Client records will be marked as inactive, and not be available to be accessed. Any Partner Agency information will remain in the system but will be marked as inactive.
3) The Partner Agency must return all hardware (firewalls, etc.) that is owned by Bitfocus.
4) Any fees paid for participation in the SCC HMIS will not be refunded.
5) The Partner Agency understands and accepts any ramifications of not participating in the SCC HMIS.

Involuntary Removal: It is vital for the County and Bitfocus to provide a secure service for all users. Any action(s) that threaten the integrity of the system will not be tolerated.

1) Bitfocus reserves the right to modify, limit, or suspend any user account at any time if there is a security risk to the system.
2) Any improper use of the SCC HMIS is subject to immediate suspension of the user's account. The penalties imposed on a user for improper system use will vary based on the level of the offense. Typically the user will receive a warning upon the first offense. However, if the offense is severe enough, Bitfocus reserves the right to disable the account immediately and, in extreme cases, to disable all users' access at the Partner Agency in question.
3) Bitfocus will contact the Partner Agency within one business day of any such suspension.
4) If a user's account is suspended, only the Technical Administrator for a Partner Agency may request account re-activation. Suspended users may be required to attend additional training before having their access reinstated.
5) In the event that a Partner Agency is removed from the system, it must submit a written request for reinstatement to the SCC HMIS Working Group and Bitfocus. If the Partner Agency is not reinstated into the system after review of its reinstatement request, the Partner Agency will be given one copy of its data in a format that will be determined by Bitfocus and approved by the SCC HMIS Working Group. (The Partner Agency will also be provided with a description of the data format.) Data will not be given to the Partner Agency until all hardware (firewalls, etc.) belonging to Bitfocus is returned. Any fees paid for participation in the SCC HMIS will not be returned.

Section 16: Additional Participation Standards

System/Data Security: In the event a Partner Agency becomes aware of a system security or client confidentiality breach, the Partner Agency's Security Officer shall notify the HMIS System Administrator of the breach within one business day.

SCC HMIS related forms and printed material: The Partner Agency agrees to maintain all Client Consent to Data Collection and Release of Information forms, and all Client Revocation of Consent forms, related to the SCC HMIS for 6 years after expiration. This documentation may be requested by the County, Bitfocus, or its contractors for the purposes of periodic audits.

Destruction of SCC HMIS related printed material: Any SCC HMIS forms or printed information obtained by a Partner Agency or user from the SCC HMIS system must be destroyed in a manner that ensures client confidentiality will not be compromised.

Section 17: No Third-Party Beneficiaries

These SOPs have been set forth solely for the benefit and protection of the County, Bitfocus, and the respective Partner Agencies and their respective heirs, personal representatives, successors and assigns. No other person or entity shall have any rights of any nature in connection with or arising from these SOPs. Without limiting the generality of the preceding

sentence, no user of the SCC HMIS in his or her capacity as such and no current, former, or prospective client of any Partner Agency shall have any rights of any nature in connection with or arising from these SOPs.

Section 18: Data Quality Procedures

Data must be entered according to the timeliness and completeness guidelines provided in the *Continuous Data Quality Improvement Process* document, a copy of which is attached as Appendix F.

Section 19: Anti-Snooping Policy

Snooping is an inappropriate access and a serious HIPAA violation. HMIS Users are prohibited from accessing records of co-workers, friends, neighbors & family members. Snooping fines range from $25,000 - $250,000 per incident.

Section 20: Electronic Customer Portal Access

The Customer Portal ("The Portal") is software that connects clients to SCC HMIS. Authorized clients may access a portion of their HMIS Record through the Customer Portal.

Identity Verification: Prior to sending a portal invitation the client identity and contact information will be verified by the Partner Agency. Clients will be required to share their full date of birth in HMIS prior to accessing the portal. To verify client identity agencies should ask for the individual's full name and confirm two identifying pieces of information. Identifying information may include: date of birth, contact phone number or address, social security numbers, photo, recent service history, HMIS id number, or other individualized information in the client record. Agency staff will verify the client email listed on the Contact tab in Clarity matches the Email registered to the portal account.

Authorized Access: Only the individual identified in the client record is authorized to access the Customer Portal account. Individuals must be aged 18 or older to access the Customer Portal. If the Customer Portal account is accessed by any unauthorized individual the account should be immediately deactivated. Accounts may be reinstated once the client identity and credentials are verified. An authorized individual may request to have their portal account deactivated at any time.

Portal Information and Communication: Partner Agency Staff will respond to direct messages, requests, and information sent through the Customer Portal in a timely manner. Partner agency staff will review and update information entered through the portal to ensure an accurate and complete client record. Information entered through the Portal is identified in Clarity with a portal icon.

Appendix A: List of Santa Clara County Policy Documents

Document	Version History	Date Updated
Client Consent for Data Collection and Release of Information (ROI)	Version 2020-03-11	2020Mar11
Client Grievance Form	v1.1	2016Nov08
Continuous Data Quality Improvement Process	v1.1	2015Sep16
HMIS Governance Charter	v1.1	2019Apr19
Partner Agency Privacy and Data Sharing Agreement (MOU)	Version 2015-09-14	2015Sep24
Partner Agency Technical Administrator and Security Officer Agreement	Version 2015-09-25	2015Sep25
End User Agreement	v.2020	2020Jan15
Standard Operating Procedures (SOPs) Includes: • HMIS Client Grievance Procedures • HMIS Privacy Statement • HMIS Security Plan • HMIS Quarterly Compliance Certification Checklist	v1.1	2020Jul07

Appendix B: Quarterly Compliance Checklist

SANTA CLARA COUNTY HMIS QUARTERLY COMPLIANCE CERTIFICATION CHECKLIST	☐ Quarter 1	HMIS Partner Agency Name :	
	☐ Quarter 2		
	☐ Quarter 3	Security Officer Name:	
	☐ Quarter 4	Date:	

Workstation Security Standards

In partnership with Santa Clara County, Clarity Human Services Software, a division of Bitfocus, Inc., administers the County's Homeless Management Information System ("HMIS"), a shared database software application which confidentially collects, uses, and releases client-level information related to homelessness in the County. Client information is collected in the HMIS and released to nonprofit housing and services providers (each, a "Partner Agency," and collectively, the "Partner Agencies"), which use the information to improve housing and services quality. Partner Agencies may also use client information to identify patterns and monitor trends over time; to conduct needs assessments and prioritize services for certain homeless and low-income subpopulations; to enhance inter-agency coordination; and to monitor and report on the quality of housing and services. This Compliance Certification Checklist is to be completed and certified quarterly by the Partner Agency Security Officer for the HMIS Partner Agency named above according to the schedule outlined below. Each Agency workstation used for HMIS data collection, data entry, or reporting must be certified compliant. Any identified compliance issues must be resolved within thirty (30) days. Upon completion, the original signed copy of this checklist should be retained in the records of the HMIS Partner Agency named above for a minimum of seven (7) years. Additionally, a copy should be made available the SCC Bitfocus System Administration team (the "Lead Security Officer") at Clarity Human Services Software, a division of Bitfocus, Inc.

Compliance Certification Schedule:

- Quarter 1 (due the week of April 1): Workstation names* beginning A-F
- Quarter 2 (due the week of July 1): Workstation names beginning G-M
- Quarter 3 (due the week of October 1): Workstation names beginning N-T
- Quarter 4 (due week of January 1): Workstation names beginning U-Z

*The workstation name should be the staff first name for individual workstations or the location name for shared workstations

Checklist Items

For the purposes of the following Workstation Security Standards, "Authorized Person" means a Partner Agency authorized agent or representative (each, an "HMIS End User," or simply an "End User") who has completed the SCC HMIS Client Consent training within the past twelve (12) months.

1. An HMIS Privacy Statement is visibly posted at each HMIS intake desk (or comparable location). If the workstation is not in a fixed location HMIS Privacy Statement must be provided as a handout.

2. Each HMIS workstation computer is in a secure location where only Authorized Persons have access.
3. Each HMIS workstation computer is password-protected and locked when not in use. (Changing passwords on a regular basis is recommended)
4. Documents printed from HMIS are sent to a printer in a secure location where only Authorized Persons have access.
5. Non-authorized persons are unable to view any HMIS workstation computer monitor.
6. Each HMIS workstation computer has antivirus software with current virus definitions (i.e., within the past twenty-four (24) hours), and each HMIS workstation computer has had a full system scan within the past week.
7. Each HMIS workstation computer has and uses a hardware or software firewall.
8. Unencrypted protected personal information ("PPI") – defined as client-level identifying information, including, without limitation, information about names, birth dates, gender, race, social security number, phone number, residence address, photographic likeness, employment status, income verification, public assistance payments or allowances, food stamp allotments, or other similar information – has not been electronically stored or transmitted in any fashion (including, without limitation, by hard drive, flash drive, email, etc.). (Encrypted hard drives are recommended)
9. Hard copies of PPI (including, without limitation, client files, intake forms, printed reports, etc.) are stored in a physically secure location.
10. Each HMIS workstation computer password information, including each Authorized Person's user identification information, is kept electronically and physically secure.

Please Note: For each of the items (1-10) be sure and mark with an (x) indicating the item is in compliance in the table below.

Security Officer Workstation Checklist

Instructions: For each HMIS workstation at your agency fill in the workstation location or end username. Verify items 1 through 10 on the previous page for the workstation and check the box to confirm the verification is complete. Fill in additional notes/comments and compliance issues as needed. Attach additional pages if necessary.

Return this form to scc-admin@bitfocus.com

#	Workstation Location or End Username	1	2	3	4	5	6	7	8	9	10	Notes/Comments
1												
2												
3												
4												
5												
6												
7												

8												
9												
10												
11												
12												
13												
14												
15												
16												
17												
18												
19												
20												
21												
22												
#	**Workstation security compliance issues identified**	**Steps taken to resolve workstation security compliance issue**										

Security Officer Certifications

(Initials) I have verified that:

_____ Each End User is using the most current versions of the Santa Clara County HMIS Client Consent to Data Collection and ROI and the Partner Agency list.

_____ Each Partner Agency End User has been instructed to read and sign the Santa Clara County HMIS End User Agreement, which is viewed electronically in Clarity Human Services the first time a user logs into the system.

_____ Each Partner Agency End User has completed Santa Clara County HMIS Client Consent Training within the past twelve (12) months.

_____ Each Partner Agency End User requires access to HMIS to perform her or his assigned duties.

_____	_____	_____/____/_____
Partner Agency Security Officer Name	*Partner Agency Security Officer Signature*	*Date*

Appendix C: Sample HMIS Privacy Statement

SANTA CLARA COUNTY
HMIS PRIVACY STATEMENT

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.

The County of Santa Clara is working with other government agencies and community based organizations to run a program to improve housing and services in Santa Clara County. The program is called the Santa Clara County Homeless Management Information System ("SCC HMIS"). This Privacy Statement describes how _____ may use and disclose information that you agree to share with the HMIS program. Some examples of information you may agree to share includes your name, birth date, gender, race, social security number, phone number, residence address, photo, and other similar identifying information. You may also agree to share financial information (such as your employment status, income verification, public assistance payments or allowances, food stamp allotments, and other similar financial information, as well as medical, mental health, and substance abuse information. Before your information can be shared in the HMIS system you will be asked to give permission to enter and share your information by signing a document call the Client Consent to Data Collection and Release of Information. The Agency you share your information with may be required to collect some information about you by law or by funders of the Agency's programs.

The Agency will not collect enter information about you in the HMIS system without your written consent. The Agency will use and release the information you agree to share to do the following things:

1. Verify your eligibility and the order in which you're referred for services;
2. Provide you with or refer you to services that meet your needs;
3. Manage and evaluate the performance of its programs;
4. Report on program operations and outcomes to funders of its programs or apply for additional funding to support the program serving you or other programs;
5. Collaborate with other local agencies to improve services in Santa Clara County; or
6. To research better ways to provide services in Santa Clara County.

This agency may also be required to release your information for the following reasons:

1. When the law requires it; or,
2. When a judge, law enforcement agency, or administrative agency issues an order.

You have the right to revoke your consent by submitting a written and signed request to revoke your consent to:

Bitfocus, Inc.
ATTN: SCC HMIS
548 Market Street #60866
San Francisco, CA 94104

Consent may be revoked verbally for records relating to drug/alcohol treatment or mental health treatment by calling Bitfocus at (408) 596-5866.

You also have the following rights:

1. You have the right to inspect and to have a copy of all the information collected about you and included in the HMIS system;
2. You have the right to an explanation about the HMIS system and any information that you do not understand;
3. You have the right to request a correction of inaccurate or incomplete information about you in the HMIS system. Your request may be denied pursuant to applicable law or at the Agency's discretion, but your request will be noted in the program records;
4. Restrictions on the type of information released to other Agencies; and,
5. A current copy of this Privacy Statement.

All agents and representatives of the Agency with access to your information are required to complete formal training on the system and the privacy requirements at least annually.

This Privacy Statement may be amended at any time. Amendments may effect information obtained by the Agency before the date of the change. An amendment to this Privacy Statement regarding use or release of information will be effective with respect to information processed before the amendment, unless otherwise stated.

All questions and requests related to this Privacy Statement should be directed to:

Name and Title of Agency Security Officer or Privacy Officer
Partner Agency Street Address
City, State, Zip
Phone
Email

Appendix D: Sample Client Grievance Form

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 Santa Clara County CoC Board 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 deliver the form to Bitfocus, Inc. via US Mail at:

Bitfocus, Inc.
548 Market St #60866
San Francisco, CA 94104

If you have any questions about completing this form, please call (408) 596-5866 and ask to speak with the Santa Clara County HMIS System Administrator.

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.

Please sign and date below:

_____ _____
Client Signature Date

Appendix E: Client Revocation of Consent to Release Information

Clarity - Homeless Management Information System

Client Revocation of Consent to Release Information

I hereby revoke permission for the partner agencies in the Santa Clara County Continuum of Care to share my personal information and information regarding my family in the Homeless Management Information System (HMIS). I understand that my information will remain in HMIS as part of the non-identifying data collected on homeless services provided by the Continuum of Care, but that my personal and family information will no longer be available to any partner agency.

_____ _____

Client Name (please print) Client Signature Date

_____

Client Unique Identifier

Executed At:

_____

Name of Partner Agency

_____ _____

Agency Personnel Name (print) Agency Personnel Signature Date

Comments:

(Comments and ideas from clients and case workers are encouraged):

Appendix F: Continuous Data Quality Improvement Process

Continuous Data Quality Improvement Process
Santa Clara Continuum of Care

Data Quality Defined

Data quality is a term that refers to the reliability and validity of client-level in HMIS. It is measured by the extent to which data in the system reflects actual information in the real world. With good data quality, a Continuum of Care can accurately tell its story of the individuals and families it serves.

Overview of Data Quality Continuous Improvement Process

A continuous data quality improvement process facilitates the ability of the CoC to achieve statistically valid and reliable data. It sets expectations for both the community and the end users to capture reliable and valid data on persons accessing your agency's programs and services.

Roles & Responsibilities

Bitfocus will provide the following services to assist agencies in correctly entering data in HMIS, and in addressing data quality issues:

- Provide end user trainings and workflow documents.
- Work with agency management to identify at least one agency employee as an HMIS agency administrator.
- Produce data quality reports and information on how to correct any identified data quality issues.
- Provide technical assistance to agencies requesting assistance in identifying what steps need to be taken in order to correct data quality issues
- Provide other services as contracted with a CoC and/or agency.

Agencies will take primary responsibility for entering, verifying, and correcting data entry:

- Agency staff will measure completeness by running APRs and other reports, then distribute those reports to staff tasked with improving data completeness
- It is the responsibility of Agency management to ensure staff tasked with correcting data quality issues do so in a timely manner.

Data Quality Standards

There are three general types of programs, each with a set of data elements that are required for every adult client. All required elements, regardless of program type, must have 0% Null rates. Don't Know and Refused rates vary by program.

Timeline

Data quality reports should be run at least once per month throughout the year. In the weeks prior to submitting a report (e.g.: AHAR), data quality reports may need to be run on a daily basis.

Data Completeness

No Null (missing) data for required data elements. Don't Know or Refused responses should not exceed the allowed percentages (see below for details).

TH, PSH, & RRH Programs

Data Element	Applies to:	Don't Know/Refused Should Not Exceed
First Name	All Clients	5%
Last Name	All Clients	5%
SSN	All Clients	n/a
Date of Birth	All Clients	5%
Race	All Clients	n/a
Ethnicity	All Clients	5%
Gender	All Clients	5%
Veteran Status	Adults Only	5%
Disabling Condition	Adults Only	5%
Residence Prior to Program Entry	Adults & HoHH	5%

Zip Code of Last Permanent Address	All Clients	5%
Housing Status (at entry)	Adults & HoHH	5%
Income and Sources (at entry)	Adults & HoHH	5%
Income and Sources (at exit)	Adults & HoHH Leavers	5%
Non-Cash Benefits (at entry)	Adults & HoHH	5%
Non-Cash Benefits (at exit)	Adults & HoHH Leavers	5%
Physical Disability	All Clients	5%
Developmental Disability	All Clients	5%
Chronic Health Condition	All Clients	5%
HIV/AIDS	All Clients	5%
Mental Health	All Clients	5%
Substance Abuse	All Clients	5%
Domestic Violence	Adults & HoHH	5%
Destination	Adults & HoHH Leavers	5%

Outreach and Emergency Shelter

Data Element	**Applies to:**	**Don't Know/Refused Should Not Exceed**
First Name	All Clients	5%
Last Name	All Clients	5%
SSN	All Clients	n/a
Date of Birth	All Clients	5%

Race	All Clients	n/a
Ethnicity	All Clients	5%
Gender	All Clients	5%
Veteran Status	Adults Only	5%
Disabling Condition	Adults Only	5%
Residence Prior to Program Entry	Adults & HoHH	5%
Zip Code of Last Permanent Address	All Clients	5%
Housing Status (at entry)	Adults & HoHH	5%
Income and Sources (at entry)	Adults & HoHH	5%
Income and Sources (at exit)	Adults & HoHH Leavers	5%
Non-Cash Benefits (at entry)	Adults & HoHH	5%
Non-Cash Benefits (at exit)	Adults & HoHH Leavers	5%
Physical Disability	All Clients	5%
Developmental Disability	All Clients	5%
Chronic Health Condition	All Clients	5%
HIV/AIDS	All Clients	5%
Mental Health	All Clients	5%
Substance Abuse	All Clients	5%
Domestic Violence	Adults & HoHH	5%
Destination	Adults & HoHH Leavers	30%

Minimizing Data Quality Issues

How you can minimize data quality issues:

- Enter client data as soon as possible. The more time passes between collecting data and entering the data in HMIS, the greater the odds there will be data quality issues.
    - Recommended Time Frames:
        - Transitional and Permanent Housing Programs: Enter all program entry/exit data within three (3) workdays.
        - Emergency Shelters and non-HUD: Enter check in/checkout within one (1) workday
        - Outreach: Create client profile, if necessary, within three (3) workdays. Record outreach services within one (1) workday.
- Whenever possible, consider entering data during client visits so that clients may help identify potential inaccuracies.
- Review Data Quality using APRs at least once a month. Correct all null values as soon as possible.

When to Correct Data Quality Issues

At a minimum, you should begin correcting data quality issues should least two (2) months before a report is submitted to the agency requesting the report.

In general, you should evaluate and correct data quality quarterly using the following schedule:

- First month of quarter: begin data quality review, focused on ensuring the correct number of clients are enrolled and there are no null values. Make corrections as needed. For example, ensure that no required information, such as veteran status, is missing.
- Second month of quarter: review data with relevant program managers and/or staff to verify accuracy of data compared other records. For example, ensure that veteran status data entered into Clarity is correct.
- Third month of quarter: assess agency workflow to identify process improvements that may help ensure high quality data is consistently entered into system.

Correcting Data Quality Issues

The following reports can help identify the majority of data quality issues:

- [HUDX-227] Annual Performance Report
- [HUDX-225] HMIS Data Quality Report
- [DQXX-110] Duplicate Clients
- [DQXX-103] Monthly Staff Report
- [DQXX-102] Program Data Review
- [DQXX-105] Monthly Agency Utilization Report

Longitudinal Systems Analysis (LSA)

The Longitudinal Systems Analysis (LSA) report, produced from a CoC's Homelessness Management Information System (HMIS) and submitted annually to HUD via the HDX 2.0, provides HUD and Continuums of Care (CoCs) with critical information about how people experiencing homelessness use their system of care (HUD Exchange, 2018).

Preparation includes:

- Updated bed inventory reflecting inventory from the previous 2 years for RRH projects.
- Review household enrollments to ensure all enrollments have the same HoH from Project Start to Project Exit.
- Ensure Organization Names is the full legal name of the agency.
- Verify project zip codes with Providers.

Annual Performance Review (APR)

Preparation and submission schedule:

- Two (2) Months before due date: begin data quality review, focused on ensuring the correct number of clients are enrolled and there are no null values. Make corrections as needed. For example, ensure that no required information, such as veteran status, is missing.
- One (1) Month before due date: review data with relevant program managers and/or staff to verify accuracy of data compared other records. For example, ensure that veteran status data entered into Clarity is correct.
- Two (2) weeks before due date: enter data into esnaps.
- One (1) week before due date: conduct internal review of data entered into esnaps to verify accuracy