King County

King County Homeless Management Information System (HMIS)

STANDARD OPERATING POLICIES

The King County HMIS is a shared database and software application that confidentially collects, uses, and shares client-level information related to homelessness in King County. HMIS is designed to capture comprehensive and timely information about services supporting persons and families who are at risk of or experiencing homelessness in King County and to measure results and outcomes of those services. The goals of HMIS are to:

- Ensure accurate data about the nature of homeless services and clients in King County;
- Ensure accurate data about the nature and extent of prevention services provided to households at risk of homelessness in King County;
- Assist in facilitating a coordinated system of care for homeless and at risk populations;
- Collect data that fulfills federal, state and local requirements for homeless reporting; and
- Provide client information capacity to facilitate potential collaborative information collection and service development and provision initiatives.

These Standard Operating Policies ("SOPs") outline the foundation for system security including the policy for access to the system, the data for export, import or data analysis needs, and physical system access, as well as the procedures for maintaining the system and data integrity.

Section 1: Contractual Requirements and Mandatory Roles

On behalf of the Seattle/King County Continuum of Care ("CoC"), HMIS is administered by King County Department of Human and Community Services ("County") in a software application called Clarity Human Services ("Clarity"), a product of Bitfocus, Inc. ("Bitfocus"). The County has also contracted with Bitfocus to serve as the System Administrator for the HMIS.

The Continuum of Care System Performance Committee, staffed by All Home, is designed to support data collection and evaluation efforts for the Seattle/King County Continuum of Care in order to assess and inform progress on ending homelessness.

<u>As the HMIS Lead, the County is responsible for:</u>

- Assuring that the Seattle/King County CoC remains in compliance with federal regulations including the HEARTH Act of 2009, the HMIS Requirements Proposed Rule of 2011, and the most recent version of the HMIS Data Standards.
- Assuring that the HMIS is administered and operated under high standards of data

quality and security including the appropriate collection, maintenance, use, disclosure, transmission, assuring records retention policies are followed, and the maintenance of privacy, security, and confidentiality protections.

- Assure all HMIS ROIs, Agreements, Security Plan, and Policies and Procedures Manuals as up to date and as needed approved by the System Performance Committee.

- Assure reports are submitted to HUD and Department of Commerce as required.

- Oversight of the HMIS System Administrator and ensuring the software comply with HMIS standards issued by HUD.

As the System Administrator, Bitfocus is responsible for:

- Developing and implementing an annual HMIS Work Plan and Continuous Data Quality Improvement Plan.

- Providing system administration & project management to facilitate and coordinate all activities in the implementation and operation of HMIS. This includes development and ongoing implementation of HMIS standards and operating procedures, communicating with Partner Agencies and coordinating activities on behalf of King County.

- Providing ongoing technical support services to Partner Agencies and Users to fully utilize the features of HMIS. Technical support provides data quality assessment, help-desk phone support, help-desk email support, help-desk live chat, and any additional support necessary to assure the successful operation of HMIS.

- Provide basic to advanced ongoing training services in a variety of applicable formats (Webinar, Video, Knowledge Base, Website, Print Manual, Classroom) in order to ensure that Users are able to utilize the system. More information can be found in the Training and User Support Plan.

The Continuum of Care System Performance Committee is responsible for:

- Informing the administration of the HMIS, including developing the vision for HMIS and approving the HMIS System Administrator annual work plan;

- Reviewing the daily operations and strategic initiatives for HMIS to support consistent participation in HMIS and positive user experience and support;

- Reviewing and approving policies for the HMIS, including privacy mechanisms, security plan, data quality plan, and the HMIS Partner Agency Privacy and Data Sharing Agreement and data sharing agreements; and

- Reviewing on a quarterly basis the outcomes of any submitted requests to share client-level data made to King County during that time period.

HMIS Partner Agencies are responsible for:

- Executing a Partner Agency Privacy and Data Sharing Agreement and a Partner Agency Technical Administrator and Security Officer Agreement.

- Assigning Agency staff to the following roles (as defined in Appendix A) in order for the agency to begin using HMIS (Note: More than one role may be assigned to the same individual):

  - ❑ Partner Agency HMIS Lead / Technical Administrator
  - ❑ Partner Agency Security Officer
  - ❑ Partner Agency Intake Worker or Case Manager or End User

  In addition, some Partner Agencies may also have the following roles:

  - ▫ Partner Agency Mental Health Worker
  - ▫ Partner Agency Substance Abuse Counselor
  - ▫ Partner Agency Health Worker
  - ▫ Partner Agency Data Analyst
  - ▫ Continuum of Care Representative
  - ▫ Continuum of Care Evaluator
  - ▫ Contract monitor

- Assuring the standards outlined in the HMIS Security Plan are followed. 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.

Section 2: Participation Requirements

Participation Policy: Agencies that are funded as part of the Seattle / King County Continuum of Care to provide homeless programs and/or services will be required to participate in the HMIS. All other homeless providers are strongly encouraged to participate in the HMIS. There is a complete list of the King County HMIS Policies in Appendix B.

Participation Requirements: For the most efficient utilization of the services provided by the 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 HMIS Partner Agency Technical Administrator to serve as the primary contact, or the name of an outside contractor;

- Completion of a network and site security assessment to comply with the most recent version of 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) and the HMIS Partner Agency Technical Administrator And Security Officer Agreement;

- Adopting written policies concerning client consent for release of information, client grievance procedures, data security procedures, data beach procedures, and interview protocols as specified in this document.

Section 3: Stages of Implementation

Stage 1 – Startup: Partner Agencies must complete all MOUs and agreements, and adopt all policies and procedures required in these SOPs.

- HMIS Partner Agency Privacy and Data Sharing Agreement

- HMIS Partner Agency Technical Administrator And Security Officer Agreement

Stage 2 – Organization Data Entry: Partner Agencies must define the organization and provide detailed descriptions of programs and eligibility, as well as define user workflow. All programs set up in HMIS are subject to King County approval.

Stage 3 – Initial System Rollout: Partner Agencies must ensure that privacy and confidentiality training is completed by Technical Administrators, Security Officers, and all End Users. They must also define users and responsibilities. All HMIS training be conducted using a demonstration version of the software and data. Real client data will **NEVER** be used for training purposes.

Stage 4 – Client Data Entry: Partner Agencies begins entering client information into the HMIS.

Stage 5 – Client-Program Entry: Partner Agencies begins entering client use of their programs.

Stage 6 – Case Management: Partner Agencies may use the HMIS as a case management tool in the day-to-day operation of the agencies if such agencies wish to do so.

Stage 7 – Program Management: Partner Agencies may use the HMIS to track program performance on an agency level.

Section 4: User, Location, Physical and Data Access

Access Privileges to the 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 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 HMIS will be categorized. Access to data sets, types of data, and all other information housed as part of the HMIS is governed by policies approved by the System Performance Committee and the County. Reproduction, distribution, destruction of, and access to the data are based on the content of the data.

Client Consent Required. Per the Partner Agency Privacy and Data Sharing Agreement at no time may identifying confidential data be distributed or accessible without the consent of the client(s) in question[1]

Computers and Electronic Devices: Security for data maintained in HMIS depends on a secure computing environment. 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 should be used. All access to HMIS should be in compliance with the HMIS Security Plan. Also see the Accessing HMIS in the Field: A Practical Guide for Agencies for more information about best practices.

Connecting to the Clarity Human Services Application: Bitfocus, Inc. uses a Two-Factor Authentication (2FA) solution to ensure that only approved users have access to HMIS data and the Clarity Human Services application. The 2FA system consists of: (1) an emailed code or authenticator app code to verify user on trusted device in order to access Clarity; and (2) a username and password issued by Bitfocus.

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 HMIS name, or the 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

[1] **Re-release Prohibited:** Agency agrees not to release any Client identifying information received from HMIS to any other person or organization without written informed Client consent, or as required by law. Any other requests for information from or related to HMIS should be sent to Bitfocus and the County. The Agency is encouraged to seek its own legal advice if required by law to provide identifying confidential client information.

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: King County has the right to suspend, limit, or revoke the access of any Partner Agency or individual for violation of HMIS policies, including these SOPs. Upon remedy of a proven violation, access rights may be reinstated. If privileges have not been reinstated, the Partner Agency or individual may file an appeal to the System Performance Committee for reinstatement.

Monitoring: Access to the HMIS will be monitored. In addition, the 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 quarterly 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: Data Quality Procedures

Data quality is a term that refers to the reliability and validity of client-level data 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 the story of the individuals and families it serves.

Data Quality Improvement Plan

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 end users for capturing reliable and valid data on persons accessing agency programs and services.

The Continuous Data Quality Improvement Plan contains an overview of the improvement process, data quality standards, guidance on minimizing data quality issues, and the data use schedule with reporting timelines.

Data Quality Monitoring

On a monthly basis, the HMIS Partner Agency Technical Administrator will receive a Monthly Staff Report by email, which will summarize for each individual user and across the agency as a whole: (1) the percentage of "client refused" values; (2) the percentage of "client doesn't know" values; and (3) the percentage of "data not collected" values. Agencies are expected to review the report and take action to ensure that their agency-level "Client Refused," "Client Doesn't Know," and "Data Not Collected" values do not exceed 5%. On a quarterly basis, Bitfocus will monitor data completeness and follow up with agencies who exceed 5% in any of the categories listed above as described below:

> *Support Step 1*: As result of regular data quality reviews that are aligned with the Data Quality Improvement Plan, if an agency is found to be out of data quality compliance, Bitfocus staff will notify the HMIS Partner Agency Technical Administrator and identify

data quality concerns and/or errors that need to be fixed. Technical assistance will be available by phone or in person to resolve the data entry difficulties. Agency staff will be expected to acknowledge Bitfocus communication and comply with deadlines.

Support Step 2: If the agency continues to be out of compliance after three outreach attempts by Bitfocus, the Executive Director may be notified and the agency may be required to submit a written action plan to Bitfocus outlining corrective steps. Bitfocus will share the corrective action plan with the King County, City of Seattle or United Way representatives who oversee the agency contracts, and will report monthly to the System Performance Committee on the status and progress of all corrective action plans.

Support Step 3: Failure to correct actions and/or continuation of unresolved data quality issues will result in a potential funding suspension notice issued by the HMIS funding partners.

Data Timeliness Requirements

Data must be entered according to the timeliness guidelines below

Program Type	Data Timeliness Standard: At Entry	Data Timeliness Standard: At Exit
Emergency shelter	All Universal Data Elements and Program-Specific Data Elements entered within two business days of intake	**Night by Night**: All Universal Data Elements and Program-Specific Data Elements entered at or before 30 calendar days after last service date. Exit date backdated to last service **Entry/Exit**: All Universal Data Elements and Program-Specific Data Elements entered within two business days of exit
Transitional Housing	All Universal and Program-Specific Data Elements entered within two business days of intake	All Universal and Program-Specific Data Elements entered within two business days of exit
	All Universal and Program-Specific Data Elements	All Universal and Program-Specific Data Elements

Permanent Supportive Housing	entered within two business days of intake	entered within two business days of exit
Homelessness Prevention	All Universal and Program-Specific Data Elements entered within two business days of intake	All Universal and Program-Specific Data Elements entered within two business days of exit
Service only	All Universal and Program-Specific Data Elements entered within two business days of intake	All Universal and Program-Specific Data Elements entered within two business days of exit
Outreach	All Universal and Program-Specific Data Elements entered within two business days of intake	All Universal and Program Specific Data Elements entered at or before 30 calendar days after last service date. Exit date backdated to last service
Day Centers	All Universal and Program-Specific Data Elements entered within two business days of intake	All Universal and Program Specific Data Elements entered at or before 30 calendar days after last service date. Exit date backdated to last service (Day Center Enrollments without any activity will be automatically exited 90 days after last service date.)

<u>Data Completeness Requirements</u>

The purpose of data completeness requirements are to ensure that our community has the ability to produce accurate unduplicated counts of people served and to fully understand the demographic characteristics and service patterns of clients accessing homeless and prevention services.

- All Clients Served: 100% of clients in HMIS-participating programs have a record entered in HMIS.
- Universal Data Elements: All programs have 95% complete data for the Universal Data Elements.* Complete data does not include missing, 'Don't know' or 'Refused'

answers. For anonymized clients the following data elements will be exempted from the 95% completeness standard: (1) Social Security Number: (2) first name; (3) last name; (4) date of birth. For large-scale night-by-night shelters, lower targets for data completeness will be considered based on past performance.

- Program Specific Data Elements: All programs have 95% complete data for the Program Specific Data Elements. Complete data does not include missing, 'Don't know' or 'Refused' answers. For large-scale night-by-night shelters, lower targets for data completeness will be considered based on past performance.
- Bed Utilization Rate: Bed Utilization in HMIS accurately reflects the number of people being served on a given night. The general standard for bed utilization is between 85% and 105%. All bed nights must be recorded within 2 business days for night-by-night shelters. For entry/exit shelters, TH, and PSH programs, entering entry and exit dates within two business days will ensure accurate occupancy rates."

* Clients who cannot complete these fields for legal reasons (i.e. those experiencing domestic violence or having a protected HIV status) will not count against the 95% data completeness standard.

Section 6: Training

In collaboration with King County and other key partners, Bitfocus, Inc. provides current information and training about best practices for using Clarity Human Services software and relevant updates to meet funder expectations. Ongoing training helps to ensure data accuracy, user satisfaction, and high quality client services.

1. **User, Client Privacy, and Basic Security Training:** Bitfocus will provide training to instruct all HMIS users in the proper procedures to operate 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.

2. **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 or meeting offered specifically for Technical Administrators and/or Security Officers. Such training will take place in King County, Washington or by webinar. When offered, these trainings or meetings will cover practical problem solving strategies needed to improve the operation or security of the HMIS.

3. **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. 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.

Specific training information will be documented in the annual King County HMIS Training and User Support Plan.

Section 7: Technical Support and System Availability

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

2. Partner Agency Service Requests: System administrative staff is only permitted to respond to service requests that are submitted in writing by the Partner Agency Executive Director or on-site Technical Administrator or Security Officer, or by Partner Agency staff authorized to make such requests.

3. Rapid Response Technical Support: The Bitfocus helpdesk phone 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. The helpdesk is only available during business hours, so the Partner Agencies should plan accordingly.

4. 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 8: Partner Agency Meetings

Partner Agency meetings will be scheduled periodically with advance notice given via the HMIS email distribution list. The Bitfocus staff responsible for HMIS matters will 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.

More details are provided in Bitfocus' annual King County HMIS Training and User Support Plan.

Section 9: Data Release Protocols

Collection of Client Identified information

An agency shall collect client identified information only when appropriate to the purposes for which the information is obtained or when required by law. An Agency must collect client information by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.

1. The Agency will use the Client Consent to Data Collection and Release of Information form, describing how client information may be collected, used, and released by the County and the CoC in the administration of the HMIS. Only the standard, County-issued Client Consent to Data Collection and Release of Information form may be used.
2. The Agency must maintain appropriate documentation of informed client consent, in writing and signed by each client, to participate in the HMIS. All documentation must be provided to the County within ten (10) days upon request.

Obtaining Client Consent

In obtaining client consent, each adult Client in the household must sign the approved King County HMIS Client Consent to Data Collection and Release of Information form to indicate consent to enter Client identified information into HMIS. If minors are present in the household, at least one adult in the household must consent minors by writing their names on the Client Consent to Data Collection and Release of Information form. If any adult member of a household does not provide written consent, identifying information may not be entered into HMIS for *anyone* in the household. Unaccompanied youth aged 13 or older may consent to have their personally identifying information entered in HMIS.

1. Do not enter personally identifying information into HMIS for clients who are in licensed domestic violence agencies (Victim Service Providers) or currently fleeing or in danger from a domestic violence, dating violence, sexual assault or stalking situation.

2. Do not enter HIV/AIDS status in HMIS. If funding (i.e., HOPWA) requires HMIS use, those clients' data shall be entered without personally identifying information.

More information can be found in the ROI Frequently Asked Questions document.

Documenting Client Consent in HMIS

Partner Agencies must document a client's consent status in HMIS as "Yes" or "No", and uploading the signed *HMIS Client Consent to Data Collection and Release of Information* for each member of the household, as outlined in the HMIS User Manual.

Revoking Consent

A Client may withdraw or revoke consent for Client identified information collection by signing the Client Revocation of Consent form. The Agency will follow King County's policies for creating de-identified clients and all non-identifying information for the client shall be entered into the HMIS.

A Client may revoke consent by providing written revocation of consent to Bitfocus at the following address:

Bitfocus, Inc.
ATTN: King County HMIS
5940 S Rainbow Blvd Ste 400 #60866
Las Vegas, Nevada 89118-2507

If a Client revokes their consent, Agency is responsible for obtaining a Client Revocation of Consent form signed by the client, keeping the form on file and available for review, and immediately contacting the HMIS System Administrator (Bitfocus Inc) at: kcsupport@bitfocus.com or 206.444.4001 x2 to have the client record de-identified according to King County's policies.

Consent may be revoked verbally for records pertaining to drug/alcohol treatment, and for records where client is actively fleeing domestic violence. If consent is revoked verbally to the Agency, the Agency will inform Bitfocus of such revocation immediately.

The Agency is prohibited from removing identified information from HMIS directly but is responsible for notifying Bitfocus Inc and the CEA program to ensure that Client can be contacted for a housing referral if applicable.

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 Consent Refuse Data Entry Protocol listed below.

1. Start with Quality of Name field and enter "Client Refused"
2. Enter zeros for SSN
3. Change to "Client Refused" for Quality of SSN
4. Type "Refused" for Last Name
5. Type "Consent" for First Name
6. Enter 01/01/ and up or down a year or two for Date of Birth
7. Enter "Client Refused" 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. Copy the new "Unique Identifier" field that now appears with an auto-filled number, and paste that into the First Name field, eliminating the word "Consent." Alternately, use your Alternate Client ID to replace the word "Consent" in First Name. 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.

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.

The Client Consent for Data Collection and Release of Information (ROI) form will be a dated document with a defined term. The Partner Agency 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. Also, the client can revoke his or her consent at any time and have his or her file deidentified,

by signing a Client Revocation of Consent form or 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.

Continuum Approved Uses and Disclosures

1. Agency shall be responsible for complying with all HMIS policies and procedures, and for establishing and maintaining the HMIS Security Plan that is designed to ensure the security and confidentiality of the data from HMIS to which Agency has access. This includes protection against any anticipated threats or hazards to the security or integrity of HMIS data, and protection against unauthorized access to or use of HMIS Data that could result in substantial harm or inconvenience to the County or any client or HMIS user.

2. The Agency will utilize the HMIS as part of the Coordinated Entry for All (CEA) system in accordance with the CEA Standard Operating Policies. Use of HMIS for CEA includes, but is not limited to, entering data for the approved CEA tools in order to place clients into the priority pool for referral to housing programs, and accepting referrals for clients from the Coordinated Entry for All system.

3. Agency will not access identifying information for any individual for whom services are neither sought nor provided by the Agency.
4. If the Agency wishes to share information from HMIS beyond information related solely to services provided by the Agency, it must first inform and receive approval from the County as the HMIS lead.
5. Agency will use HMIS database for legitimate business purposes only.
6. Agency will not use HMIS in violation of any federal or state law, including, but not limited to, copyright, trademark and trade secret laws, and laws prohibiting the transmission of material, which is threatening, harassing, or obscene.
7. Agency will not use the HMIS database to defraud federal, state or local governments, individuals or entities, or conduct any illegal activity.

Section 10: HMIS 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.

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 King County HMIS website: kingcounty.hmis.cc. A copy of the form is included in Appendix D. 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 County. The System Performance Committee will be notified of all grievances received. Bitfocus will use its reasonable best efforts to investigate the issue and will inform the System Performance Committee of the results.

If the issue is not system related, the System Performance Committee 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 System Performance Committee.

Section 11: Participation without using Clarity Human Services software (data integration)

If a Partner Agency wishes to participate in the HMIS through data integration the following additional guidelines must be met:

1. The Partner Agency must obtain authorization from King County to participate via data integration. At this time King County is honoring historic commitments around data integration but is not allowing new agencies to participate via data integration;

2. The Partner Agency understands that it is its responsibility to pay for any additional costs related to feeding data to the HMIS;

3. The Partner Agency must be able to produce an extract file from its existing system;

4. The Partner Agency must be able to produce the extract file in a format specified by Bitfocus and approved by King County DCHS;

5. The Partner Agency understands that the extract format will most likely change in the future. The Partner Agency agrees to adapt their data integration processes within 30 days of an updated format becoming available in HMIS;

6. The Partner Agency data imported into the HMIS will be available for all purposes for which HMIS data may be legitimately used, including but not limited to, generating aggregate reports and identifying the service history of specific clients;

7. If, at a later date, a Partner Agency chooses to use the Clarity Human Services software, the agency understands that some or all of its historical imported data may not be available; and

8. Some parts of Sections 1 – 8 of this SOP document may not apply to Partner Agencies entering data into the HMIS system via the data integration method.

9. Partner Agencies interested in replicating HMIS data into a non-HMIS data system must obtain permission from King County and must pay for any additional costs related to the replication process.

10. All data synchronized through data replication is subject to all provisions of this SOP document pertaining to client privacy, consent, and use of data.

NOTE: For programs that are part of coordinated entry (CEA), data integration will be possible only AFTER a client has been enrolled into a program that participates in CEA. The coordinated entry and referral tools in Clarity must be used by all agencies participating in CEA up to the point a client is enrolled into a program (which is how referrals are accepted in Clarity) or a referral is denied. The coordinated entry/referral tools include:

- Updating program availability
- Viewing referrals sent to partner agencies by referral specialists
- Indicating when referrals are in process
- Denying referrals
- Accepting referrals by enrolling a client into the program to which they were referred

In the event that data integration isn't available, agencies are responsible for direct entering all data related to CEA in a timely manner. There are no exceptions to this policy.

Agencies participating in data integration must meet the following data timeliness standards. Additional data timeliness standards as described in Section 5 must also be met.

Program Type	Data Timeliness Standard
Emergency shelter	All Universal and Program-Specific Data Elements will be uploaded weekly
Transitional Housing	All Universal and Program-Specific Data Elements will be uploaded weekly
Permanent Supportive Housing	All Universal and Program-Specific Data Elements will be uploaded weekly
Homelessness Prevention	All Universal and Program-Specific Data Elements will be uploaded weekly
Service only	All Universal and Program-Specific Data Elements will be uploaded weekly

Section 12: Additional Participation Standards

Coordinated Entry

The Agency shall utilize HMIS as part of the CoC's Coordinated Entry for All system in accordance with the CEA Operations Manual, and aligned with the HMIS Data and Technical Standards at (CoC Program interim rule) 24 CFR 578.7(a)(8).

An individual client has a right to adequate notice of a CEA Partner Agency's use and release of Personally Identifying Information (PII) and of the individual's rights in regards to data about them, as well as the Partner Agency's legal duties with respect to PII.

Whether a households consents to having their information in HMIS or not, their PII will be shared in order to make a referral for housing and services

The CEA Privacy Statement is read by the CEA Housing Assessors before a CEA Housing Triage Tool is completed and should be prominently displayed or distributed in the program offices where the CEA Housing Triage Tool is completed.

The CEA Coordinating Entity will promptly revise and redistribute the CEA 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.

A non-consenting client may also request that their PII not be shared for the purposes of a housing or service referral through CEA, this will result in the client being removed from the CEA priority list. This request can be send to cea@kingcounty.gov with subject line removal for CEA Priority List.

Partner Agencies understand that they are prohibited from penalizing or threatening to penalize clients for either revoking their previously provided written consent or requesting that their information be held in the strictest confidence.

The following privacy statement must be prominently displayed:

> *Completing the CEA Housing Triage Tool allows Coordinated Entry for All (CEA) to make referrals on your behalf to Partner Agencies for housing and services. The only information shared with Partner Agencies will be for the purpose of coordinating a housing or service referral. Partner Agencies receiving a housing or service referral from CEA will be provided your name and contact information. A complete list of Partner Agencies can be found in the CEA Operations Manual found on the CEA website.*

Section 13: No Third-Party Beneficiaries

These SOPs have been set forth solely for the benefit and protection of the System Performance Committee, 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 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.Appendix A: HMIS Partner Agency Roles

- The *Partner Agency HMIS Technical Administrator* is the primary point of contact between Bitfocus and the Partner Agency.

- 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.

- The *Partner Agency Security Officer* will conduct semi-annual compliance reviews and ensures that all End Users complete required trainings. A semi-annual compliance checklist form entitled "King County HMIS Semi-Annual Compliance Certification Checklist" is available on the King County HMIS website as noted in Appendix B.

- The *Partner Agency Intake Worker* is able to create client files and run reports at the agencies) where they work; 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 *Partner Agency Case Manager* 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 *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 *Partner Agency Mental Health Worker* 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 generated in that agency.

- The *Partner Agency Substance Abuse Counselor* 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 and able to view sensitive portions of the record generated in that agency.

- The *Partner Agency Health Worker* 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 and able to view sensitive portions of the record generated in that agency.

- The *Partner Agency 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 Evaluator* is able to view aggregate-level reports, demographics, service utilization, total statistics and numbers regarding data in the system

- The *Contract Monitor* 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.

Appendix B: List of King County HMIS Policy Documents

Document	Date Updated
Agency Desk Sign	1April2016
Client Consent for Data Collection and Release of Information (ROI)	12Nov2018
Client Grievance Form	11July2016
Client Information Sheet	8Apr2016
Client Revocation of Consent Form	12Nov2018
Continuous Data Quality Improvement Process	31Jan2017
HMIS Governance Charter	7Sep2016
HMIS User Policy, Responsibility Statement and Code of Ethics	1Apr2016
Partner Agency Privacy and Data Sharing Agreement	12Nov2018
Partner Agency Technical Administrator and Security Officer Agreement	12Nov2018
Standard Operating Policies (SOPs)	2Jun2017
Training and User Support Plan	10Feb2017
Security Plan	12Nov2018

HMIS Client 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

In partnership with King County, Clarity Human Services Software, a division of Bitfocus, Inc. ("Bitfocus"), administers the County's Homeless Management Information System ("HMIS"), a shared database software application that confidentially collects, uses, and releases client-level information related to homelessness in the County.

This Partner Agency Privacy Statement (the "Privacy Statement") describes how _____ (the "Partner Agency," or simply the "Agency"), may use and disclose clients' Personally Identifiable Information ("PII"), including identifying information (such as client name, birth date, gender, race, social security number, phone number, residence address, photographic likeness, and other similar identifying information) and financial information (such as client employment status, income verification, public assistance payments or allowances, food stamp allotments, and other similar financial information).

The Agency may be required to collect some PII by law or by funders of the Agency's programs. The Agency may choose to collect other PII to improve housing or services quality; 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.

The Agency will not collect PII without a client's written consent in the form of one or more signed Client Consent for Data Collection and Release of Information (ROI) form(s).

The Agency will only use and/or release client PII to:

1. Verify client eligibility for services;
2. Provide client services or refer clients to services that meet their 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 its programs;
5. Collaborate with other local agencies to improve service coordination, reduce gaps in services, and develop community-wide strategic plans to address basic human needs; and/or

The Agency may also be required to release client PII for the following reasons:

1. When the law requires it;

2. When necessary to prevent or respond to a serious and imminent threat to health or safety; and/or

3. When a judge, law enforcement agency, or administrative agency issues an order.

The Agency will use and release client PII to the minimum extent necessary to effect authorized purposes, Use and release of client PII other than those described above will not be made without each client's written consent. Clients have the right to revoke their consent by signing a Client Revocation of Consent form or submitting a written and signed request to revoke their consent. In emergency situations, such as domestic violence, clients may revoke consent verbally to Agency staff.

All Clients have the right to request in writing:

1. A copy of all PII collected;

2. Any change to any PII used to make decisions about their care and services (provided, however, that such a request may be denied at the Agency's discretion, in which case the client's request will be noted in the program records);

3. An account of all releases of client PII;

4. Restrictions on the type of information released to other Partner Agencies; and

5. A current copy of the Agency's Privacy Statement and a record of all amendments made hereto.

The Agency reserves the right to refuse client's written requests described in the paragraph immediate preceding this one under any of the following circumstances:

1. The information responsive to the client's request was or is being compiled in reasonable anticipation of litigation or comparable proceedings;

2. The record responsive to the client's request includes information about another individual (other than a health care or homeless services provider);

3. The information responsive to the client's request was obtained under a promise of confidentiality (other than a promise from a health care or homeless services provider) and release of such information would reveal the source of the information; or

4. The Agency reasonably believes that release of the information responsive to the client's request would result in the endangerment of the life or physical safety of any individual.

If a client request is denied, the client will receive a written explanation of the reason for such denial. Additionally, the client will have the right to appeal the denial by following Agency grievance procedures. Regardless of the result of the appeal, the client has the right to add to your records a concise statement of disagreement. The Agency will release such statement of disagreement whenever it releases the disputed PII to another individual or entity.

All agents and representatives of the Agency with access to your PII are required to complete formal training in privacy requirements.

This Privacy Statement may be amended at any time. Amendments may affect 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 obtained before the amendment, unless otherwise stated.

This Privacy Statement reflects the basic requirements of the most recent version of 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. To the extent that this Privacy Statement is not consistent with HUD's basic requirements described above, HUD's requirements will control.

King County Homeless Management Information System (HMIS)

CLIENT GRIEVANCE FORM

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 King County System Performance 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 deliver the form to Bitfocus, Inc. via US Mail at:

Bitfocus, Inc.

5940 S Rainbow Blvd Ste 400, #60866

Las Vegas, Nevada 89118-2507

If you have any questions about completing this form, please call (206) 444-4001 and ask to speak with the King County HMIS System Administrator.

King County

King County 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: HMIS User Policy, Responsibility Statement and Code of Ethics Completed electronically upon each users first log into Clarity

USER POLICY

HMIS User Policy, Responsibility Statement and Code of Ethics

USER POLICY

Partner Agencies who use the Homeless Management Information System (HMIS) and each User within any Partner Agency are bound by various restrictions regarding Client information.

It is a Client's decision what personal information, if any, is entered into the HMIS. The Client Release of Information and Informed Consent form ("Client Release of Information") shall be signed by the Client before any identifiable Client information is entered into the HMIS. User shall insure that, prior to obtaining the Client's signature, the Client Release of Information form was fully reviewed with the Client in a manner reasonably calculated to ensure the client understood the information, and User will verify that the Client has had the opportunity to ask questions and that steps were taken as needed to assist the client in fully understanding the information. (e.g.: securing a translator if necessary).

USER CODE OF ETHICS

Users must be prepared to answer Client questions regarding the HMIS.

Users must faithfully respect Client preferences with regard to the entry and sharing of Client information within the HMIS. Users must accurately record Client's preferences by making the proper designations as to sharing of Client information and/or any restrictions on the sharing of Client information.

Users must allow the Client to opt in or out of releasing information for entry into the HMIS and changes to his/her information sharing preferences upon request. The Client Revocation of Consent form must be on file if the Client revokes consent to share his or her personal data.

Users must not refuse services to a Client, or potential Client, if that Client refuses to allow entry of personal information into the HMIS or to share personal information with other agencies via the HMIS.

The User has primary responsibility for information entered by the User. Information that Users enter must be truthful, accurate and complete to the best of User's knowledge.

Users will not solicit from, or enter information about, Clients into the HMIS unless the information is required for a legitimate business purpose, such as providing services to the Client, and/or is required by the program funder.

Users will not use the HMIS database for any violation of any law, to defraud any entity or to conduct any illegal activity.

Upon Client written request, Users must allow a Client to inspect and obtain a copy of the Client's own information maintained within the HMIS. Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding need not be provided to the Client.

Users must permit Clients to file a written complaint regarding the use or treatment of their personal information within the HMIS. Client may file a written complaint with either the Agency or the Department of Commerce – Housing Assistance Unit, HMIS Administrator at PO Box 42525, Olympia, WA 98504-2525. Client will not be retaliated against for filing a complaint.

USER RESPONSIBILITY

Your username and password give you access to the HMIS. Users are also responsible for obtaining and maintaining their own security certificates in accordance with the Agency Partner Agreement. All Users will be responsible for attending a Washington State Department of Commerce (Commerce) approved

training class prior to their first use of the HMIS. Furthermore, all Users will be expected to attend a Commerce approved training class at least once every other year to ensure their understanding and acquisition of new material pertaining to the HMIS.

Please place a check in each box below to indicate your understanding and acceptance of the proper use of HMIS access. READ CAREFULLY. Failure to uphold the confidentiality standards set forth below is grounds for immediate termination from HMIS access and may result in disciplinary action from the Partner Agency as defined in the Partner Agency's personnel policies.

Please read these statements carefully.

I agree to maintain the confidentiality of Client information in the HMIS in the following manner:

- My username and password are for my use only and will not be shared with anyone.
- I will read and abide by the HMIS Client Release of Information
- I will not use the browser capacity to remember passwords. I will enter the password each time I open HMIS.
- I will take reasonable means to keep my password physically secure.
- I will only view, obtain, disclose, or use the database information that is necessary to perform my job.
- I understand that the only individuals who may directly access HMIS Client information are authorized Users.

To prevent casual observers from seeing or hearing HMIS Client information:

- I will log off the HMIS before leaving my work area.
- I will not leave any computer or electronic device that has the HMIS "open and running" unattended.
- I will keep my computer monitor or electronic device positioned so that persons not authorized to use the HMIS cannot view it.
- I will not transmit confidential client information in email form.
- I will store hard copies of HMIS information in a secure file and not leave such hard copy information in public view on my desk, on a photocopier, printer or fax machine.
- I will properly destroy paper copies of HMIS information when they are no longer needed unless they are required to be retained in accordance with applicable law. (RCW 40.14.060)
- I will not discuss HMIS confidential Client information with staff, Clients, or Client family members in a public area.
- I will not discuss HMIS confidential Client information on the telephone in any areas where the public might overhear my conversation.
- I will not leave messages on my agency's answering machine or voicemail system that contains HMIS confidential Client information.
- I will keep answering machine volume low ensuring HMIS confidential information left by callers is not overheard by the public or unauthorized persons
- I will not transmit client identifying information via email.
- I understand that a failure to follow these security steps appropriately may result in a breach of Client HMIS confidentiality and HMIS security. If such a breach occurs, my access to the HMIS may be terminated and I may be subject to further disciplinary action as defined in the partner agency's personnel policy.
- If I notice or suspect a security breach, I will immediately notify the Director of my Agency and the Department of Commerce.

I understand and agree to comply with all the statements listed above:

_____

User Policy & Code of Ethics_v4 Revised June 5, 2018

This form may not be amended except by approval of the Washington State Department of Commerce

Approved as to form by Sandra Adix, Assistant Attorney General, June 5, 2018