King County HMIS
Standard Operating Procedures

Section 1: Contractual Requirements and Mandatory Roles

Bitfocus, Inc. Contractual Requirements: Bitfocus, Inc. ("Bitfocus"), in its role as King County HMIS ("HMIS") System Administrator, agrees to 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 provide technical assistance related to the use of Clarity Human Services software, relevant hardware, and adherence to HMIS policies and procedures, including HUD requirements, to all participating housing and services providers (the "Partner Agencies"). Additional services may be provided on a case-by-case basis, as agreed upon by Bitfocus and a Partner Agency.

Contractual Requirements for Central Server: 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 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.

HMIS Steering Committee Role: The HMIS has a steering committee (the "HMIS Steering Committee," or simply the "Steering Committee") to govern the project. The group is composed of representatives of stakeholders. These include, agencies funded by the U.S. Department of Housing and Urban Development ("HUD"), homeless services providers, local governments, and other funders. The procedures for the qualifications and meetings of members of the HMIS Steering Committee, and related matters, shall be set forth in the HMIS Governance Charter of the HMIS Steering Committee, which may be amended from time to time according to the terms therein.

Central Server Management Roles: Management of an HMIS requires several skill sets. The Steering Committee has identified the following roles to provide the best and most efficient service to HMIS stakeholders:

- 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; and supervises personnel.
- Report Writer/Technical Assistant/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, going on-site if necessary to resolve software issues.

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 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 HMIS Lead
- Partner Agency 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

Note: More than one role may be assigned to the same individual.

The *Partner Agency HMIS Lead* 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 is attached as 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.

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.

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 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) or other applicable agreement(s);
- 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.

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.

Confidentiality and Consent Forms: Partner Agencies must use the forms approved by the HMIS Steering Committee. 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 11 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 completed general Clarity Human Services user training prior to being authorized to use the system. In addition, all users of the system are required to attend confidentiality and privacy training.

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 an exception has been granted by King County.

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 King County.

Section 3: Training

User, Client Privacy, and Basic Security 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 King County, Washington 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. 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 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 HMIS Steering Committee 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 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.

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) a unique security certificate issued to each user by Bitfocus and installed on equipment or devices (e.g. computers) used to access Clarity; and (2) a username and password issued by Bitfocus.

Public Key Infrastructure Security Certificates:
Bitfocus, Inc. will use an enhanced authentication system, issuing security certificates to every user by email. The user must download and install the certificate. Bitfocus will also send each user instructions for retrieving a unique password used in the certificate installation process.

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 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 HMIS Steering 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: 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 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 Executive Director or on-site Technical Administrator or Security Officer.

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

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 other 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 must begin entering client information into the HMIS.

Stage 5 – Client-Program Entry: Partner Agencies must begin 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 7: Encryption Management

Encryption General: All information should be encrypted in the database per HUD standards. All connections to the 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 HMIS Steering Committee must obtain the written authorization of every Partner Agency's Executive Director.

Section 8: Data Release Protocols

Data Entry: Before any data will be entered into the 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 only enter the information into the system that has been approved by the client. The HMIS will assign the client a unique personal identifier. Partner Agencies should note that services must not be contingent on a client consenting to data entry.

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.

Basic Consent Refused Client Record Data Entry Protocol

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 "Approximate" for Quality of DOB
8. Enter a unique ID in Alternate Client ID so you can come back to this client and find them again(or leave it blank. if you want the system number to be there instead). If you do fill it in, please make sure it is not in and of itself containing personal information
9. Enter Gender, Race, Ethnicity and perhaps Veteran status with real data if it won't serve to identify them in any way
10. Leave Middle Name and Suffix blank
11. Click Add Record
12. In the "Unique Identifier" field that now appears with an auto-filled number, copy and paste that into the Alternate Client ID field (if you don't want to make up your own) and 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.

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 participating agencies should 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). All ROI forms that were valid and officially approved for use by the HMIS Steering Committee at the time they are signed by a client will be accepted.

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 HMIS Client Information: The Partner Agency must notify Bitfocus 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.

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, in full or in part, and have his or her file deactivated, 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: 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 Participating Agency. "Disclosures" involve sharing parts of client information with persons or organizations outside of an HMIS Participating 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 *King County Homeless Management Information System (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.

Releases of anonymous client-level data for research purposes must be approved by the HMIS Steering Committee. Aggregate data must meet appropriate data quality and coverage 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 King County Security Plan includes the following elements: (1) designated security officers; (2) semi-annual 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.

King County Lead Security Officer

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.

Partner Agency Security Officer:

1. May be the HMIS Partner Agency Technical Administrator or another Partner Agency employee, volunteer or contractor who has completed HMIS Privacy and Security training 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 semi-annual 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 Semi-Annual 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 King 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.

Semi-Annual Partner Agency Self-Audits

1. The Partner Agency Security Officer will use the HMIS Semi-Annual Compliance Certification Checklist to conduct semi-annual 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 1 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 semi-annual 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 Semi-Annual 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 1 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 Privacy and Security 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. Non-HMIS trained staff will need to receive training that incorporates all of the privacy and confidentiality requirements in this SOP document. Alternatively, non-HMIS staff may attend a 30-minute privacy and security training that will be offered by Bitfocus
2. Printer location – Documents printed from HMIS must be sent to a printer in a secure location where only authorized persons have access. HMIS-trained and non-HMIS trained staff may use the same computers. Non-HMIS trained staff will need to receive

training that incorporates all of the privacy and confidentiality requirements in this SOP document. Alternatively, non-HMIS staff may attend a 30-minute privacy and security training that will be offered by Bitfocus

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. The HMIS Lead Agency will enlist the use of PKI (Public Key Infrastructure) or another suitably secure method to identify approved workstations, in compliance with Public Access baseline requirement in the HUD Data Standards. The Partner Agency Security Officer will verify that a current PKI certificate (available from the HMIS System Administrator) has been installed on each End User's workstation.
3. 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).
4. Partner Agency Security Officer will confirm that any workstation accessing HMIS has and uses a 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 HMIS Privacy, Security and Ethics training and End User Responsibilities and Workflow training, prior to being provided with a User ID to access HMIS.
3. All End Users will be issued a unique User ID and password by Bitfocus. Sharing of User IDs and passwords by or among more than one End User is expressly prohibited. Each End User must be specifically identified as the sole holder of a User ID and password. User IDs and passwords may not be transferred from one user to another.
4. The HMIS Partner Agency Technical Agency Administrator will always attempt to approve the most restrictive access that allows the End User to efficiently and effectively perform his/her assigned duties.
5. The HMIS Partner Agency Technical Administrator will notify Bitfocus when new users are approved for usernames and passwords.
6. The HMIS Partner Agency Technical Administrator will notify Bitfocus which access level to assign to each authorized user. Access levels may vary across HMIS Partner Agencies, depending upon their involvement with coordinated entry, contract monitoring, program and system evaluation, and other factors.
7. When the HMIS Partner Agency Technical Administrator determines that it is necessary to change a user's access level, the Partner Agency HMIS Partner Agency Technical Administrator will notify Bitfocus as soon as possible.

Other Technical Safeguards

1. The HMIS Partner Agency 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.

Rescinding User Access

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.

5. King County is empowered to permanently revoke a Partner Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the King 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 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. Participating agencies are required to run and maintain their own antivirus software from an approved source on all computers that have access to the HMIS system.

Operating System Updates: The goal will be to update or patch the 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 HMIS on a daily basis. In addition, backups will be stored electronically offsite. A backup of hardware and 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 off site systems for viability twice per year.

Community Reporting Process: At the direction of the King County, Bitfocus will publish community-wide aggregate reports or dashboards summarizing information about the clients in the HMIS on a periodic basis. These report(s) or dashboard(s) will reflect raw, point-in-time data.

Termination of the HMIS system: In the event the 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 central server will be purged or stored. If the latter occurs, the data will remain in an encrypted and aggregate state.

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

Section 11: 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 all HMIS Steering Committee members. The HMIS Steering Committee will be notified of all grievances received. Bitfocus will use its reasonable best efforts to investigate the issue and will inform the HMIS Steering Committee of the results.

If the issue is not system related, the HMIS Steering 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 HMIS Steering Committee.

Section 12: HMIS Privacy Statement

An individual client has a right to adequate notice of a Partner Agency's use and release of PPI and of the individual's rights in regards to data about them, 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 client's written authorization and that the individual may revoke such authorization.

- A statement of the individual client'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 Privacy Statement 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)

If a Partner Agency wishes to participate in the HMIS, but does not wish to use the Clarity Human Services software, the following additional guidelines must be met:

1. The Partner Agency must obtain authorization from King County 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 the HMIS Steering Committee;

5. The Partner Agency understands that the extract format will most likely change in the future (one of the main reasons for the file format change is that there is a movement underway to standardize the HMIS import file formats);
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. Sections 1 – 8 of this SOP document do not apply to Partner Agencies entering data into the HMIS system.
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.

If a Partner Agency wishes to integrate data into HMIS and meets all of the requirements in Section 12 listed above:

1. The agency must meet with Bitfocus to discuss and address all details of data sharing (for example, what information is to be shared, the direction of sharing, etc.);
2. The Agency must execute a Partner Agency Privacy and Data Sharing Agreement (MOU)
3. Partner Agencies must comply with Section 8 of this document (relating to obtaining clients' permission to have their information shared).

Section 14: User Meetings

User meetings will be scheduled periodically with advance notice given via the HMIS mailing list and posted on the King County HMIS website: kingcounty.hmis.cc. The Bitfocus staff responsible for HMIS matters will be available to confer with participating 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 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 HMIS understands the following:

1. The Partner Agency will receive one copy of the data it has input into the HMIS. Such copy will be in a format determined by Bitfocus and approved by the HMIS Steering Committee. 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. The client's program 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 HMIS will not be refunded.
5. The Partner Agency understands and accepts any ramifications of not participating in the HMIS, including impacts on coordinated entry (among other things).

Involuntary Removal: It is vital for the King 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 or remove any Partner Agency at any time if there is a security risk to the system.
2) Any improper use of the 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 Executive Director (or acting Executive Director) 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 HMIS Steering Committee 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 HMIS Steering Committee. (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 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 Executive Director or Security Officer shall notify the HMIS System Administrator of the breach within one business day.

HMIS related forms and printed material: The Partner Agency agrees to maintain all completed Client Consent for Data Collection and Release of Information (ROI) and Client Revocation of Consent forms, related to the HMIS. When appropriate, this documentation may be stored in Clarity Human Services. This documentation may be requested by the HMIS Steering Committee, Bitfocus, or its contractors for the purposes of periodic audits.

Destruction of HMIS related printed material: Any HMIS forms or printed information obtained by a Partner Agency or user from the 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 HMIS Steering 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.

Section 18: Data Quality Procedures

Data must be entered according to the timeliness guidelines below

Direct Entry Agencies

Program Type	Data Timeliness Standard
Emergency shelter	All Universal Data Elements entered within two business days of intake
Transitional Housing	All Universal and Program-Specific Data Elements entered within two business days of intake

Permanent Supportive Housing	All Universal and Program-Specific Data Elements entered within two business days of intake
HPRP	All Universal and Program-Specific Data Elements entered within two business days of intake
Service only	All Universal and Program-Specific Data Elements entered within two business days of intake

Data Integration Agencies

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
HPRP	All Universal and Program-Specific Data Elements will be uploaded weekly
Service only	All Universal and Program-Specific Data Elements will be uploaded weekly

Data Completeness

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 preventions services.

Standard: All data entered into HMIS is complete

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. For households that do not complete

Program Specific 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 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 50% and 105%.

* Clients who are undocumented and/or 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.

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: If an agency is found to be out of data quality compliance, Bitfocus staff will notify the HMIS Partner Agency Technical Administrator in writing within 2 business days. Technical assistance will be available by phone or in person to resolve the data entry difficulties. Agency staff will have 5 business days to correct the issue.

Support Step 2: If the agency is out of compliance a second time within three months or continues to be out of compliance, the Executive Director will be notified and the agency will 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 HMIS Steering Committee on the status and progress of all corrective action plans.

Support Step 3: A third episode of non-compliance within six months or continuation of unresolved data quality issues will result in a potential funding suspension notice issued by the HMIS funding partners.

Support Step 4: A fourth episode of non-compliance or continuing issues of data quality deficiency within six months will result in agency funding being suspended.

Appendix A: List of King County Policy Documents

Document	Version History	Date Updated
Agency Desk Sign	v1.1	1April2016
Client Consent for Data Collection and Release of Information (ROI)	v1.3	30Mar2016
Client Grievance Form	v1.1	11July2016
Client Information Sheet	v1.4	8Apr2016
Client Revocation of Consent Form	v1.1	31Mar2016
HMIS Governance Charter	v1.1	Date adopted
HMIS User Policy, Responsibility Statement and Code of Ethics	v.1.1	1April2016
Partner Agency Privacy Privacy and Data Sharing Agreement (MOU)	v1.1	25Apr2016
Partner Agency Technical Administrator and Security Officer Agreement	v1.1	6May2016
Standard Operating Procedures (SOPs) Includes: ● HMIS Client Grievance Procedures ● HMIS Privacy Statement ● HMIS Security Plan ● HMIS Semi-Annual Compliance Certification Checklist	v1.1	9Aug2016

KING COUNTY HMIS SEMI-ANNUAL COMPLIANCE CERTIFICATION CHECKLIST

HMIS Partner Agency Name:		Security Officer Name:
Semi-Annual: July ☐	Semi-Annual: January ☐	Date:

Workstation Security Standards

In partnership with King 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 semi-annually by the Partner Agency Security Officer for the HMIS Partner Agency named above. 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 to Sara Dougherty (the "Lead Security Officer") at Clarity Human Services Software, a division of Bitfocus, Inc. (the "HMIS Lead Agency").

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 HMIS Privacy and Security training within the past twelve (12) months.

1. An HMIS Privacy Statement is visibly posted at each HMIS workstation.
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.

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

#	Workstation security compliance issues identified	Steps taken to resolve workstation security compliance issue

Data Quality Standards

1. For all data elements, less than one percent (1%) of data is null.
2. For all data elements, the rate of "Don't Know/Refused" responses is lower than the percentage established in the King County HMIS Data Quality Plan.
3. All program descriptor data elements are complete and accurately reflect program contracts and operations

#	HMIS Program Name/ID#	1	2	3	If program is not meeting standard, steps being taken to achieve compliance
1					
2					
3					
4					
5					

Security Officer Certifications

(Initials) I have verified that:

_____ Each End User is using the most current versions of the King 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 King 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 King County HMIS Privacy and Security 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*

_____ _____ _____

Partner Agency Executive Director Name *Partner Agency Executive Director Signature* *Date*

Appendix C: Sample HMIS Privacy Statement

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' protected personal information ("PPI"), 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 PPI by law or by funders of the Agency's programs. The Agency may choose to collect other PPI 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 PPI 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 PPI 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
6. Participate in research projects to better understand the needs of populations served.

The Agency may also be required to release client PPI 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 PPI to the minimum extent necessary to effect authorized purposes . Use and release of client PPI 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 PPI collected;
2. Any change to any PPI 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 PPI;
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 PPI to another individual or entity.

All agents and representatives of the Agency with access to your PPI 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.

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 King County HMIS Steering 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.
548 Market St #60866
San Francisco, CA 94104

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.

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

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 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 that has the HMIS "open and running" unattended.

 I will keep my computer monitor 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_v3 Revised 02/2014 Page 2 of 2

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, 2/3/14