COUNCIL FOR THE HOMELESS
Preventing and ending homelessness in Clark County

Homeless Management Information System (HMIS)
User Policies & Procedures

1. **Access to HMIS**
Each administrative staff and end user that an agency or the Council for the Homeless determines will have access to the database will be issued a user license, login ID, and password. Licenses and access to the database will be cancelled immediately for any staff that leaves employment with a participating agency or the County. The Agency Administrator at each Participating Agency will inform the System Administrator (SA) of staff changes within seven business days of a staff member leaving the agency. Each Participant determines the user access level for each licensed staff.
    - Client information should be accessed only in order to retrieve data relevant to a client requesting services from your agency.
    - Clients have the right to see their information on ServicePoint. If a client requests to see their information, the Participating Agency/User who receives the request must review the information with the client.

2. **Enter Data on Homeless Persons into HMIS/ServicePoint**
Adults and children who are homeless will be entered into ServicePoint. As defined by the Department of Housing and Urban Development, homeless is:

    1. An individual or family who lacks a fixed, regular, and adequate nighttime residence, meaning:
        a. An individual or family with a primary nighttime residence that is a public or private place not designed for or ordinarily used as a regular sleeping accommodation for human beings, including a car, a park, an abandoned building, a bus or train station, an airport, or a camping ground; or
        b. An individual or family living in a supervised publicly or privately operated shelter designated to provide temporary living arrangements (including congregate shelters, transitional housing, and hotels and motels paid for by charitable organizations or federal, state, or local government programs for low-income individuals); or
        c. An individual who is exiting an institution where he or she resided for 90 days or less and who resided in an emergency shelter or place not meant for human habitation immediately before entering institution;
    2. An individual or family who will imminently lose their primary nighttime residence, provided that:
        a. The primary nighttime residence will be lost within 14 days of the date of application for homeless assistance;
        b. No subsequent residence has been identified; and
        c. The individual or family lacks the resources or support networks, e.g., family friends, faith-based or other social networks needed to obtain other permanent housing;
    3. Unaccompanied youth under the 25 years of age, or families with children and youth, who do not otherwise qualify as homeless under this definition, but who:
        a. Are defined as homeless under section 387 of the Runaway and Homeless Youth Act (42 U.S.C. 5732a), section 637 of the Head Start Act (42 U.S.C. 9832), section 41403 of the Violence Against Women Act of 1994 (42 U.S.C. 14043e-2), section 330(h) of the Public Health Service Act [42 U.S.C. 254b(h)], section 3 of the Food and Nutrition Act of 2008 (7 U.S.C. 2012), section 17(b) of the Child Nutrition Act of 1966 [42 U.S.C. 1786(b)], or section 725 of the McKinney-Vento Homeless Assistance Act (42 U.S.C. 11434a);
        b. Have not had a lease, ownership interest, or occupancy agreement in a permanent housing at any time during the 60 days immediately preceding the date of application for homeless assistance;
        c. Can be expected to continue in such status for an extended period of time of chronic disabilities, or chronic physical health or mental health conditions, substance addiction, histories of domestic violence or childhood abuse (including neglect), the presence of a child or youth with a disability, or two or more barriers to employment which include the lack of a high school degree or General Education Development (GED), illiteracy, low English proficiency, a history of incarceration or detention for criminal activity, and a history of unstable employment; or
    4. Any individual or family who:
        a. Is fleeing, or is attempting to flee, domestic violence, dating violence, sexual assault, stalking, or other dangerous or life-threatening conditions related to violence against the individual or a family

member, including a child, that has either taken place within the individual's or family's primary nighttime residence or has made the individual or family afraid to return to their primary nighttime residence;
   b. Have no other residence; and
   c. Lacks the resources or support networks, e.g., family, friends, faith-based or other social networks, to obtain other permanent housing.

3. **Chronic Homeless Data will be entered into the HMIS/ServicePoint - Chronically Homeless is defined:**

   1. An individual who:
      a. Is homeless and lives in a place not meant for human habitation, a safe haven, or in an emergency shelter; and
      b. Has been homeless and living or residing in a place not meant for human habitation, a safe haven, or in an emergency shelter continuously for at least one year or on at four separate occasions in the last 3 years, where each homeless occasion was at least 15 days; and
      c. Can be diagnosed with one or more of the following conditions: substance use disorder, serious mental illness, developmental disability (as defined in section 102 of the Developmental Disabilities Assistance Bill of Rights Act of 2000 (42 U.S.C. 15002), post-traumatic stress disorder, cognitive impairments resulting from brain injury, or chronic physical illness or disability;
   2. An individual who has been residing in an institutional care facility, including a jail, substance abuse or mental health treatment facility, hospital, or other similar facility, for fewer than 90 days and met all of the criteria in paragraph (1) of this definition, before entering that facility; or
   3. A family with an adult head of household (or if there is no adult in the family, a minor head of household) who meets all of the criteria in paragraph (1) of this definition, including family whose composition has fluctuated while the head of household has been homeless.

4. **Minimum Data Entry**
   Minimum data will be entered within 3-5 working days following client contact.
   Users will request the client's signature on the Release of Information Form for each homeless or low-income client after an agency's ServicePoint startup. Data may be entered but not shared depending on the specific type of client information. The following fields are required for clients with a signed Release of Information Form:

   1. Client Profile
   2. Shelter Status including check in/check out
   3. Service Records/Referrals
   4. Entry and Exit data including all Universal Data Elements: Program entry and exit dates should be recorded at every participant's program entry or exit. Entry dates should record the first day of service or program entry with a new program entry date for each period or episode of service. Exit dates should record the last day of residence in a program's housing before the participant leaves the shelter or the last day the service was provided.

   If a client chooses not to sign a Release of Information Form, then the User will enter the client information and close this record from being shared with all other Participants.

   In the Service Record, there are certain services, referrals, and agencies not to be shared with other agencies:
   1. Domestic Violence
   2. HIV/AIDS
   3. Substance Abuse
   4. Mental Health

   This information may be released if the client signs a Release of Information.

5. **Children's Data**
   Information about clients who are under age 18 is always restricted. It is the User's responsibility to designate the information as "closed." Children's data may be shared on an "as needed" basis if a parent or guardian signs a Release of Information Form.

6. **Release of Information**
   A. Release of Information
      The Release of Information form authorizes the sharing of the Client Profile, Service Record, and Community Fields with all other ServicePoint Participants in Clark County. The client may identify certain agencies with whom his or her records will not be shared. It is the User's responsibility to secure the information as closed for specific agencies in each of the modules. **Each agency's Release of Information Form must list the HMIS system and System Administrator.** If you do not have a release of information form, the System Administrator can supply samples for your use.

   B. Release of Information
      For all sharing of other modules, the individual agency's Release of Information form will be used.

7. **ServicePoint User Group**
   The User Group will hold meetings when needed for the purpose of addressing implementation and on-going operational issues. The User Group exists for the purpose of information sharing, problem solving, and generating recommendations for the continued improvement of the local project and software upgrades. The Council for the Homeless will have continuing direct input to the on-going evolution of ServicePoint software.

8. **Technical Support**
   The Systems Administrator will be responsible for the training of all Participants in the use of ServicePoint within reasonable constraints. Bowman Internet Systems will host ServicePoint. Each Participating Agency is responsible for providing and maintaining computer hardware and Internet service.

9. **ServicePoint User Training**
   All ServicePoint Users are required to attend ServicePoint training sessions.

10. **Remote Access**
    The Agency Administrator and the System Administrator **must** approve remote access for a user. All remote access must be approved in writing and the ServicePoint Remote Access form (Attachment D) completed and signed by the Agency Administrator and the System Administrator. The System Administrator will periodically audit all remote access. Violation of confidentiality policies can result in the termination of the Agency Participation Agreement.

12. **ResourcePoint Data**
    All Participants shall provide the Systems Administrator with the complete and current ResourcePoint Data about their agency's programs and services. The Systems Administrator will initially enter this into the database, and subsequent updates will be the responsibility of each Participant.

13. **Monthly Data Upload to WA State Commerce**
    Clark County HMIS data is uploaded monthly by the HMIS administrator via secure XML files to the HMIS of WA State Commerce. The data is aggregated along with all other HMIS participating Washington counties for the purposes of state-wide reporting and combined with data from the Department of Social and Health Services (DSHS) for the purpose of analysis. Names and other identifying information are not included in any reports or publications.

14. **ServicePoint System Requirements**
    Following are the minimum system requirements for running ServicePoint for each workstation that will access the server. Minimum Workstation Requirements:

- PC with Dual Core processors (avoid using single core)
- Windows 7 and Vista – 2 Gigs minimum, XP – 1 Gig minimum of RAM
- 9GB+ hard drive (7200 rpm)
- XVGA monitor – 1024 x 768 or higher (1280 x 768 strongly advised)
- Mouse and keyboard
- Mozilla Firefox, version 26; higher or Internet Explorer, version 8.0 or 9.0; Google Chrome, version 27.0.1453.116 or higher It is recommended that your browser have 128 cipher/encryption strength installed. The browser's cache should be set to "Check for new versions of stored pages: Every visit to page.")
- Broadband Internet connection (hosted version) or LAN connection (LAN version)
- Bowman systems provided Clark County HMIS PKI security certificate must be installed by HMIS Admin to access the HMIS site.

Glossary of Homeless Management Information System Acronyms and Terms

Acronyms

AIRS – Alliance of Information & Referral Systems
AHAR – Annual Homeless Assessment Report
APR – Annual Progress Report
CHO – Covered Homeless Organization
CoC– Continuum of Care
DOB – Date of Birth
DV – Domestic Violence
ESG – Emergency Shelter Grants
FIPS – Federal Information Processing Standards Codes for states, counties, and named populated places.
HIPAA – Health Insurance Portability and Accountability Act of 1996
HMIS – Homeless Management Information System
HUD – U.S. Department of Housing and Urban Development
I&R – Information and Referral
MH – Mental Health
NOFA – Notice of Funding Availability
PIT – Point in Time
PKI – Public Key Infrastructure
PPI – Personal Protected Information
S+C – Shelter Plus Care (McKinney Vento Program)
SA – Substance Abuse
SHP – Supportive Housing Program
SRO – Single Room Occupancy
SuperNOFA – Super Notice of Funding Availability
SSN – Social Security Number
SSI – Supplemental Security Income
SSO – Supportive Services Only
TA – Technical Assistance
TANF – Temporary Assistance for Needy Families
VAWA – Violence Against Women Act
XML – Extensible Markup Language

Terms

Alliance of Information and Referral Systems **(AIRS)** – The professional association for over 1,000 community information and referral (I&R) providers serving primarily the United States and Canada. AIRS maintains a taxonomy of human services.

Annual Progress Report (APR) – report that tracks program progress and accomplishments in HUD`s competitive homeless assistance programs. The APR provides the grantee and HUD with information necessary to assess each grantee`s performance.

Audit Trail – A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Most database management systems include an audit trail component.

Bed Utilization – An indicator of whether shelter beds are occupied on a particular night or over a period of time.

Biometrics – refers to the identification of a person by computerized images of a physical feature, usually a person`s fingerprint.

Chronic homelessness – HUD defines a chronically homeless person as:

1. An individual who:
   a. Is homeless and lives in a place not meant for human habitation, a safe haven, or in an emergency shelter; and
   b. Has been homeless and living or residing in a place not meant for human habitation, a safe haven, or in an emergency shelter continuously for at least one year or on at four separate occasions in the last 3 years where each homeless occasion was at least 15 days; and

c. Can be diagnosed with one or more of the following conditions: substance use disorder, serious mental illness, developmental disability (as defined in section 102 of the Developmental Disabilities Assistance Bill of Rights Act of 2000 (42 U.S.C. 15002), post-traumatic stress disorder, cognitive impairments resulting from brain injury, or chronic physical illness or disability;

2. An individual who has been residing in an institutional care facility, including a jail, substance abuse or mental health treatment facility, hospital, or other similar facility, for fewer than 90 days and met all of the criteria in paragraph (1) of this definition, before entering that facility; or
3. A family with an adult head of household (or if there is not adult in the family, a minor head of household) who meets all of the criteria in paragraph (1) of this definition, including family whose composition has fluctuated while the head of household has been homeless.

Client Intake – The process of collecting client information upon entrance into a program.

Consumer or Client – An individual or family who has or is currently experiencing homelessness.

Continuum of Care (CoC) – A community with a unified plan to organize and deliver housing and services to meet the specific needs of people who are homeless as they move to stable housing and maximize self-sufficiency. HUD funds many homeless programs and HMIS implementations through Continuums of Care grants.

Coverage – A term commonly used by CoCs or homeless providers. It refers to the number of beds represented in an HMIS divided by the total number of beds available.

Covered Homeless Organization **(CHO)** – Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes data on homeless clients for an HMIS. The requirements of the HMIS Final Notice apply to all Covered Homeless Organizations.

Data Quality – The accuracy and completeness of all information collected and reported to the HMIS.

Data Standards – See *HMIS Data and Technical Standards Final Notice.*

De-identification – The process of removing or altering data in a client record that could be used to identify the person. This technique allows research, training, or other non-clinical applications to use real data without violating client privacy.

Digital Certificates – An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user is sending a message, is who he or she claims to be, and to provide the receiver with the means to encode a reply.

Disabling Condition – A disabling condition in reference to chronic homelessness is defined by HUD as a diagnosable substance use disorder, serious mental illness, developmental disability, or chronic physical illness or disability, including the co-occurrence of two or more of these conditions. A disabling condition limits an individual's ability to work or perform one or more activities of daily living.

Emergency Shelter – Any facility whose primary purpose is to provide temporary shelter for the homeless in general or for specific populations of the homeless.

Emergency Shelter Grant (ESG) – A federal grant program designed to help improve the quality of existing emergency shelters for the homeless, to make available additional shelters, to meet the costs of operating shelters, to provide essential social services to homeless individuals, and to help prevent homelessness.

Encryption – Conversion of plain text into unreadable data by scrambling it using a code that masks the meaning of the data to any unauthorized viewer. Computers encrypt data by using algorithms or formulas. Encrypted data are not readable unless they are converted back into plain text via decryption.

Final Notice – **See *HMIS Data and Technical Standards Final Notice***

Hashing – The process of producing hashed values for accessing data or for security. A hashed value is a number or series of numbers generated from input data. The hash is generated by a formula in such a way that it is extremely unlikely that some

other text will produce the same hash value or that data can be converted back to the original text. Hashing is often used to check whether two texts are identical. For the purposes of Homeless Management Information Systems it can be used to compare whether client records contain the same information without identifying the clients.

Homeless Management Information System (HMIS) – Computerized data collection tool designed to capture client-level information over time on the characteristics and service needs of men, women, and children experiencing homelessness.

HMIS Data and Technical Standards Final Notice – Regulations issued by HUD via the Federal Register describing the requirements for implementing HMIS. The HMIS Final Notice contains rules about who needs to participate in HMIS, what data to collect, and how to protect client information.

Inferred Consent – Once clients receive an oral explanation of HMIS, consent is assumed for data entry into HMIS. The client must be a person of age, and in possession of all his or her faculties (for example, not mentally ill).

Informed Consent – A client is informed of options of participating in an HMIS system and then specifically asked to consent. The individual needs to be of age and in possession of all of his or her faculties (for example, not mentally ill), and his or her judgment not impaired at the time of consenting (by sleep, illness, intoxication, alcohol, drugs or other health problems, etc.).

Information and Referral – A process for obtaining information about programs and services available and linking individuals or families to these services. These services can include emergency food pantries, rental assistance, public health clinics, childcare resources, support groups, legal aid, and a variety of non-profit and governmental agencies. An HMIS usually includes features to facilitate information and referral.

McKinney-Vento Act – The McKinney-Vento Homeless Assistance Act was signed into law by President Ronald Reagan on July 22, 1987. The McKinney-Vento Act funds numerous programs providing a range of services to homeless people, including the Continuum of Care Programs: the Supportive Housing Program, the Shelter Plus Care Program, and the Single Room Occupancy Program, as well as the Emergency Shelter Grant Program.

Notice of Funding Availability – An announcement of funding available for a particular program or activity. See also SuperNOFA.

Penetration Testing – The process of probing a computer system with the goal of identifying security vulnerabilities in a network and the extent to which outside parties might exploit them.

Permanent Supportive Housing – Long term, community based housing that has supportive services for homeless persons with disabilities. This type of supportive housing enables special needs populations to live independently as possible in a permanent setting. Permanent housing can be provided in one structure or in several structures at one site or in multiple structures at scattered sites.

Point in Time Inventory – A calculation of the numbers of beds in a region on one particular night.

Point in Time Count – A snapshot of the homeless population taken on a given day. Since 2005, HUD requires all CoC applicants to complete this count every other year in the last week of January. This count includes a street count in addition to a count of all clients in emergency and transitional beds.

Privacy Notice – A written, public statement of an agency's privacy practices. A notice informs clients of how personal information is used and disclosed. According to the HMIS Data and Technical Standard, all covered homeless organizations must have a privacy notice.

Program Data Elements – Data elements required for programs that receive funding under the McKinney-Vento Homeless Assistance Act and complete the Annual Progress Reports (APRs).

Public Keys – Public keys are included in digital certificates and contain information that a sender can use to encrypt information such that only a particular key can read. The recipient can also verify the identity of the sender through the sender's public key.

Scan Cards – Some communities use ID cards with bar codes to reduce intake time by electronically scanning ID cards to register clients in a bed for a night. These ID cards are commonly referred to as scan cards.

Single Room Occupancy – A residential property that includes multiple single room dwelling units. Each unit is for occupancy by a single eligible individual. The unit need not, but may, contain food preparation or sanitary facilities, or both. It provides rental assistance on behalf of homeless individuals in connection with moderate rehabilitation of SRO dwellings.

Shelter Plus Care Program – A program that provides grants for rental assistance for homeless persons with disabilities through four component programs: Tenant, Sponsor, Project, and Single Room Occupancy (SRO) Rental Assistance.

Super Notice of Funding Availability – The consolidation of all HUD's homeless grants program into one Notice of funding availability. The SuperNOFA funds the Continuum of Care Competition.

Supportive Housing Program – A program that provides housing, including housing units and group quarters that has a supportive environment and includes a planned service component.

Supportive Services – Services that may assist homeless participants in the transition from the streets or shelters into permanent or permanent supportive housing, and that assist persons with living successfully in housing.

Transitional Housing – A project that has its purpose facilitating the movement of homeless individuals and families to permanent housing within a reasonable amount of time (usually 24 months).

Unduplicated Count – The number of people who are homeless within a specified location and time period. An unduplicated count ensures that individuals are counted only once regardless of the number of times they entered or exited the homeless system or the number of programs in which they participated. Congress directed HUD to develop a strategy for data collection on homelessness so that an unduplicated count of the homeless at the local level could be produced.

Universal Data Elements – Data required to be collected from all clients serviced by homeless assistance programs using an HMIS. These data elements include date of birth, gender, race, ethnicity, veteran's status, and Social Security Number (SSN). These elements are needed for CoCs to understand the basic dynamics of homelessness in their community and for HUD to meet the Congressional directive.

Written Consent – Written consent embodies the element of informed consent in a written form. A client completes and signs a document consenting to an understanding of the options and risks of participating or sharing data in an HMIS system. The signed document is then kept on file at the agency.

Glossary Source: U.S. Department of Housing and Urban Development Office of Special Needs Assistance Programs

COUNCIL FOR THE HOMELESS
Leadership • Advocacy • Solutions

Agency Partner Agreement

Clark County HMIS

The Homeless Management Information System ("HMIS") is a client management system that maintains information regarding the characteristics and service needs of Clients for a variety of reasons, including the provision of more effective and streamlined services to Clients and the creation of information that communities can use to determine the use and effectiveness of services.

Ultimately, when used correctly and faithfully by all involved parties, the HMIS is designed to benefit multiple stakeholders, including provider agencies, people experiencing homelessness, funders and the community through improved knowledge about people who are homeless, their services and service needs and a more effective and efficient service delivery system.

The Homeless Housing and Assistance Act of 2005 requires the WA Department of Commerce to collect HMIS data in the form of a data warehouse. The Council for the Homeless ("CFTH") serves as the HMIS administrator in Clark County. Each homeless service provider will enter accurate and timely HMIS data for the Council for the Homeless, who will transmit the data to Commerce.

_____, ("Agency") has elected to participate in HMIS. Agency and Council for the Homeless agree as follows:

1. General Understandings:

a. In this Agreement, the following terms will have the following meanings:

(i) "Client" refers to a consumer of services;

(ii) "Partner Agency" refers generally to any Agency participating in HMIS.

(iii) "Agency staff" refers to both paid employees and volunteers.

(iv) "HMIS" refers to the HMIS system administered by CFTH.

(v) "Enter(ing)" or "entry" refers to the entry of any Client information into HMIS.

(vi) "Shar(e)(ing)," or "Information Shar(e)(ing)" refers to the sharing of information which has been entered in HMIS with another Partner Agency.

(vii) "Clark County CoC Steering Committee" or "Steering Committee" refers to a advisory body that serves in a consultative and counseling capacity to Council for the Homeless as the HMIS system administrator. The Steering Committee is comprised of representatives from the Continuum of Care.

(viii) "Identified Information" refers to Client data that can be used to identify a specific Client. Also referred to as "Confidential" data or information.

(ix) "De-identified Information" refers to data that has specific Client demographic information removed, allowing use of the data without identifying a specific Client. Also referred to as "non-identifying" information.

b. Agency understands that when it enters and/or extracts information in HMIS, such information will be available to CFTH staff who may review the data to administer HMIS;

Any analysis of HMIS data must be provided to CFTH FIRST to review in a timely manner, prior to any other external entity. Any reports shared externally MUST be submitted to others in de-identified form without individual identifying Client information.

c. Agency understands that Agency will have the ability to indicate whether information Agency entered into HMIS may be shared with and accessible to Partner Agencies in HMIS system. Agency is responsible for determining and designating in HMIS whether information may or may not be shared.

2. Confidentiality:

a. Agency will not:

(i) enter information into HMIS which it is not authorized to enter; and

(ii) will not designate information for sharing which Agency is not authorized to share, under any relevant federal, state, or local confidentiality laws, regulations or other restrictions applicable to Client information. By entering information into HMIS or designating it for sharing, Agency represents that it has the authority to enter such information or designate it for sharing.

b. Agency represents that: (check applicable items)

☐ it is; is not; a "covered entity" whose disclosures are restricted under HIPAA (45 CFR 160 and 164); More information about "covered entities" can be found here: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

☐ it is; is not; a program whose disclosures are restricted under Federal Drug and Alcohol Confidentiality Regulations: 42 CFR Part 2;

(iii) If Agency is subject to HIPAA, (45 CFR 160 and 164) or 42 CFR Part 2, a fully executed Business Associate or Business Associate/Qualified Service Organization Agreement must be attached to this agreement before information may be entered. Sharing of information will not be permitted otherwise.

(iv) If Agency is subject to any laws or requirements which restrict Agency's ability to either enter or authorize sharing of information, Agency will ensure that any entry it makes and all designations for sharing fully comply with all applicable laws or other restrictions.

c. Agency shall comply with the Violence Against Women and Department of Justice Reauthorization Act of 2005 (VAWA) and Washington State RCW 43.185C.030. No Identified

Information may be entered into HMIS for Clients in licensed domestic violence programs (Victim Service Providers) or for Clients fleeing domestic violence situations.

d. Agency shall not enter confidential information regarding HIV/AIDS status, in accordance with RCW 70.02.220. If funding (i.e., HOPWA) requires HMIS use, those clients' data shall be entered without Identifying Information.

e. To the extent that information entered by Agency into HMIS is or becomes subject to additional restrictions, Agency will immediately inform CFTH in writing of such restrictions.

3. **Information Collection, Release and Sharing Consent:**

a. 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.

b. Obtaining Client Consent: In obtaining Client consent, each adult Client in the household must sign the HMIS Client Release of Information 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 HMIS Client Release of Information. 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.

(i) 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.

(ii) 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.

(iii) Telephonic consent from the individual may temporarily substitute written consent provided that written consent is obtained at the first time the individual is physically present at Agency.

(iv) A Client may withdraw or revoke consent for Client identified information collection by signing the HMIS Revocation of Consent. If a Client revokes their consent, Agency is responsible for immediately contacting CFTH and making appropriate data modifications in HMIS to ensure that Client's personal identified information will not be shared with other Partner Agencies or visible to the Agency staff within the system.

(v) This information is being gathered for the collection and maintenance of a research database and data repository. The consent is in effect until the client revokes the consent in writing.

4. **No Conditioning of Services:** Agency will not condition any services upon or decline to provide any services to a Client based upon a Client's refusal to allow entry of identified information into HMIS.

5. **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.

6. **Client Inspection/Correction:** Agency will allow a Client to inspect and obtain a copy of his/her own personal information except for information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding. Agency will also allow a Client to correct information HMIS Agency Partner Agreement Agency Partner Agreement__2018_Final.DOCX Revised 06/18 Page 4 of 8 June 2018 that is inaccurate. Corrections may be made by way of a new entry that is in addition to but is not a replacement for an older entry.

7. **Security:** Agency will maintain security and confidentiality of HMIS information and is responsible for the actions of its users and for their training and supervision. Among the steps Agency will take to maintain security and confidentiality are:

a. **Access:** Agency will permit access to HMIS or information obtained from it only to authorized Agency staff who need access to HMIS for legitimate business purposes (such as to provide services to the Client, to conduct evaluation or research, to administer the program, or to comply with regulatory requirements). Agency will limit the access of such staff to only those records that are immediately relevant to their work assignments.

b. **User Policy:** Prior to permitting any user to access HMIS, Agency will require the user to sign a User Policy, Responsibility Statement & Code of Ethics ("User Policy") and is incorporated into this agreement and may be amended from time to time by CFTH. Agency will comply with, and enforce the User Policy and will inform CFTH immediately in writing of any breaches of the User Policy.

c. **Computers and Electronic Devices:** Security for data maintained in HMIS depends on a secure computing environment. Computer and device security is adopted from relevant provisions of the Department of Housing and Urban Development's (HUD) "Homeless Management Information Systems (HMIS) Data and Technical Standards Notice" (Docket No. FR 4848-N-01; see https://www.hudexchange.info/resource/1318/2004-hmis-data-and-technical-standardsfinal-notice/) until the HMIS Proposed Rule is finalized and replaces the current Standards: https://www.hudexchange.info/resource/1967/hearth-proposed-rule-for-hmisrequirements/. Agencies are encouraged to directly consult that document for complete documentation of HUD's standards relating to HMIS.

Agency agrees to allow access to HMIS only from computers and Electronic Devices which are:

- owned by Agency for the purpose of accessing and working with HMIS (no personal devices)
- Portable Electronic Devices (i.e., tablets, cell phones) may only be used for HMIS with prior written approval from CFTH.
- protected from viruses by commercially available virus protection software

- protected with a software or hardware firewall
- maintained to insure that the operating system running the computer or electronic device used for the HMIS is kept up to date in terms of security and other operating system patches, updates, and fixes
- accessed through web browsers with 256-bit encryption (e.g., Internet Explorer, version 11.0). Some browsers have the capacity to remember passwords, so that the user does not need to type in the password when returning to password-protected sites. This default shall not be used with respect to CFTH's HMIS; the end-user is expected to physically enter the password each time he or she logs on to the system HMIS Agency Partner Agreement Agency Partner Agreement__2018_Final.DOCX Revised 06/18 Page 5 of 8 June 2018
- staffed at all times when in public areas. When computers and electronic devices are not in use and staff is not present, steps should be taken to ensure that the computers, electronic devices, and data are secure and not publicly accessible. These steps should minimally include: Logging off the data entry system, physically locking the computer or electronic device in a secure area, or shutting down the computer or electronic device entirely

d. **Passwords:** Agency will permit access to HMIS only with use of a User ID and password, which the user may not share with others. Written information pertaining to user access (e.g. username and password) shall not be stored or displayed in any publicly accessible location.

   Passwords shall be at least eight characters long and meet industry standard complexity requirements, including, but not limited to, the use of at least one of each of the following kinds of characters in the passwords: Upper and lower-case letters, and numbers and symbols. Passwords shall not be, or include, the username, or the HMIS name. In addition, passwords should not consist entirely of any word found in the common dictionary or any of the above spelled backwards. The use of default passwords on initial entry into the HMIS application is allowed so long as the default password is changed on first use. Passwords and user names shall be consistent with guidelines issued from time to time by HUD and/or CFTH.

e. **Training/Assistance**: Agency will permit access to HMIS only after the authorized user receives appropriate confidentiality training including that provided by CFTH. Agency will also conduct ongoing basic confidentiality training for all persons with access to HMIS and will train all persons who may receive information produced from HMIS on the confidentiality of such information. Agency will participate in such training as is provided from time to time by CFTH. CFTH will be reasonably available during CFTH defined weekday business hours for technical assistance (i.e. troubleshooting and report generation).

f. **Records:** Agency and CFTH will maintain records of any disclosures of Client identifying information either of them makes of HMIS information for a period of seven years after such disclosure. On written request of a Client, Agency and CFTH will provide an accounting of all such disclosures within the prior seven-year period. CFTH will have access to an audit trail

from HMIS so as to produce an accounting of disclosures made from one Agency to another by way of sharing of information from HMIS.

g. **Retention of paper copies of personally identifying information:** Agencies must develop and adopt policies governing the retention of paper records containing personally identifying information derived from a Homeless Management Information system. The policy must define how long paper records are retained after they are no longer being actively utilized, and the process that will be used to destroy the records to prevent the release of personally identifying information. The policy must require the destruction of the paper records derived from an HMIS no longer than seven years after the last day the person was served by the organization.

8. **Information Entry Standards:**

a. Information entered into HMIS by Agency will be truthful, accurate and complete to the best of Agency's knowledge. HMIS Agency Partner Agreement Agency Partner Agreement__2018_Final.DOCX Revised 06/18 Page 6 of 8 June 2018

b. Agency will not solicit from Clients or enter information about Clients into the HMIS database unless the information is required for a legitimate business purpose such as to provide services to the Client, to conduct evaluation or research, to administer the program, or to comply with regulatory requirements.

c. Agency will only enter information into HMIS database with respect to individuals that it serves or intends to serve, including through referral.

d. Agency will enter all data for a particular month into HMIS database by the 5th business day of the following month. Additionally, Agency will make every attempt enter all data for a particular week by the end of that week.

e. Agency will not alter or over-write information entered by another Agency.

9. **Use of HMIS:**

a. Agency will not access identifying information for any individual for whom services are neither sought nor provided by the Agency. Agency may access identifying information of the Clients it serves and may request via writing access to statistical, non-identifying information on both the Clients it serves and Clients served by other HMIS participating agencies.

b. Agency may report non-identifying information to other entities for funding or planning purposes. Such non-identifying information shall not directly identify individual Clients.

c. Agency and CFTH will report only non-identifying information in response to requests for information from HMIS unless otherwise required by law.

d. Agency will use HMIS database for legitimate business purposes only.

e. 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.

f. Agency will not use the HMIS database to defraud federal, state or local governments, individuals or entities, or conduct any illegal activity.

10. **Proprietary Rights of the HMIS:**

a. Agency shall not give or share assigned passwords and access codes for HMIS with any other Agency, business, or individual. Each user shall request their own login and password.

b. Agency shall take due diligence not to cause in any manner, or way, corruption of the HMIS database, and Agency agrees to be responsible for any damage it may cause.

11. **Limitation of Liability and Indemnification:** No party to this Agreement shall assume any additional liability of any kind due to its execution of this agreement of participation in the HMIS. It is the intent of the parties that each party shall remain liable, to the extent provided by law, regarding its own acts and omissions; but that no party shall assume additional liability on its own behalf or liability for the acts of any other person or entity except for the acts and omissions of their own employees, volunteers, agents HMIS Agency Partner Agreement Agency Partner Agreement__2018_Final.DOCX Revised 06/18 Page 7 of 8 June 2018 or contractors through participation in HMIS. The parties specifically agree that this agreement is for the benefit of the parties only and this agreement creates no rights in any third party.

12. **Limitation of Liability.** CFTH shall not be held liable to any member Agency for any cessation, delay or interruption of services, nor for any malfunction of hardware, software or equipment.

13. **Disclaimer of Warranties.** CFTH makes no warranties, express or implied, including the warranties of merchantability and fitness for a particular purpose, to any Agency or any other person or entity as to the services of the HMIS to any other matter.

14. **Additional Terms and Conditions:**

a. Agency will abide by such guidelines as are promulgated by HUD and/or CFTH from time to time regarding administration of the HMIS.

b. Agency and CFTH intend to abide by applicable law. Should any term of this agreement be inconsistent with applicable law, or should additional terms be required by applicable law, Agency and CFTH agree to modify the terms of this agreement so as to comply with applicable law.

c. Neither CFTH nor Agency will transfer or assign any rights or obligations regarding HMIS without the written consent of either party.

d. Agency agrees to indemnify and hold CFTH and its agents and staffs harmless from all claims, damages, costs, and expenses, including legal fees and disbursements paid or incurred, arising from any breach of this Agreement or any of Agency's obligations under this Agreement.

e. This Agreement will be in force until terminated by either party. Either party may terminate this agreement at will with 20 days written notice. Either party may terminate this agreement immediately upon a material breach of this Agreement by the other party, including but not limited to the breach of the CFTH Security Policy by Agency.

f. If this Agreement is terminated, Agency will no longer have access to HMIS. CFTH and the remaining Partner Agencies will maintain their right to use all of the Client information previously entered by Agency except to the extent a restriction is imposed by Client or law.

g. Copies of Agency data will be provided to the Agency upon written request of termination of this agreement. Data will be provided on CDs or other mutually agreed upon media. Unless otherwise specified in writing, copies of data will be delivered to Agency within fourteen (14) calendar days of receipt of written requests for data copies.

Signed:

Signature		Title
Date		
Executive Director, Council for the Homeless		Date

Clark County HMIS Data Privacy, Data Security and Data Quality Plans

I. Clark County HMIS data privacy plan

Information Privacy Principle: Personal information should be acquired, disclosed, and used only in ways that respect an individual's privacy.

HMIS participating programs will request the client's signature on the Release of Information Form for each homeless or low-income client. Data may be entered but not shared depending on the specific type of client information. The following fields are required for clients with a signed Release of Information Form:

1. Client Profile
2. Shelter Status including check in/check out
3. Entry/Exit Data
4. Service Records/Referrals
5. HUD Universal Data Elements (either in the client's profile or Entry/Exit)

If a client chooses not to sign a Release of Information Form, then the User will enter the client information and close this record from being shared with all other Participants.
In the Service Record, there are certain services, referrals, and agencies not to be shared with other agencies:

1. Domestic Violence
2. HIV/AIDS
3. Substance Abuse
4. Mental Health

Note: This information may be released if the client signs a Release of Information
Confidentiality of Information: Each Participant understands that participation in the ServicePoint system will make confidential information in the Client Profile available to other Participants as outlined in the User Policies and Procedures (Agency Agreement, Attachment A). It is the responsibility of each Participant to observe all applicable laws and regulations regarding client confidentiality. Only client specific data approved for release by the client and properly recorded by the Participant shall be accessible to other Participants or made available to those Participants within reports.

Client information should be accessed only in order to retrieve data relevant to a client requesting services from a participating agency.

Clients have the right to see their information on ServicePoint. If a client requests to see their information, the Participating Agency/User who receives the request must review the information with the client.

If a Client's Release of Information Form is withdrawn by the client of a Participant, that Participant maintains an ongoing responsibility to make that client's information unavailable to all other Participants. When a Participant withdraws from the ServicePoint system the former Participant must notify the System Administrator of the withdrawal, and the System Administrator will assure that all of their clients' information in ServicePoint has been promptly closed to sharing with all other Participants.

Aggregate data may be made available by the Council for the Homeless to other entities for funding or planning purposes pertaining to providing services to the homeless. However, the data released by the Council for the Homeless must never directly identify individual clients.

If a participating agency's HMIS users are found to be in violation of this privacy plan, resulting sanctions may include suspending or revoking system privileges at the discretion of the HMIS lead agency.

II. Clark County HMIS Data Security Plan

Security for data maintained in our HMIS depends on a secure computing environment. Computer security is adapted from relevant provisions of the Department of Housing and Urban Development's (HUD) "Homeless Management Information Systems (HMIS) Data and Technical Standards Notice" (Docket No. FR 4848-N-01; see http://epic.org/privacy/poverty/hmis.pdf). Agencies are encouraged to directly consult that document for complete documentation of HUD's standards relating to HMIS. Agency will allow access to HMIS only from computers which are:

a. physically present on Agency's premises; [remote access policy (Attachment C) and ServicePoint Remote
   Access Agreement (Attachment D) is only an option with written approval of Agency and System Administrator and will be audited by the System Administrator];
b. owned by Agency; or
c. approved by Agency for the purpose of accessing and working with HMIS; and
d. protected from viruses by commercially available virus protection software;
e. protected with a software or hardware firewall;
f. authorized to access the ServicePoint HMIS website through installation of the Bowman PKI (Public Key Infrastructure certificate);
g. maintained to insure that the computer operating system running the computer used for the HMIS is kept current in terms of security and other operating system patches, updates, and fixes;
h. accessed through web browsers with 128-bit encryption [e.g., Mozilla Firefox, version 26 or higher; Internet Explorer, version 8.0 or 9.0; Google Chrome, version 27.0.1453.116 or higher. Some browsers have the capacity to remember passwords so that the user does not need to type in the password when returning to password-protected sites. If available, this default shall **not** be used with respect to HMIS; the end-user is expected to physically enter the password each time he or she logs on to the system;
i. staffed at all times when in public areas. When computers are not in use and staff is not present, steps should be taken to ensure that the computers and data are secure and not publicly accessible. These steps should minimally include: Logging off the data entry system, physically locking the computer in a secure area, or shutting down the computer entirely.

Passwords: Agency will permit access to HMIS only with use of a User ID and password which the user may not share with others. Written information pertaining to user access (e.g. username and password) shall not be stored or displayed in any publicly accessible location. All users must sign a Statement of Confidentiality included on the User Agreement (Attachment E).

Security Training and review: all users will receive security training prior to being given access to the HMIS, and that the training will reflect the policies and principles of the Continuum of Care. The HMIS Lead will complete an annual security review with participating agencies to ensure the implementation of the security requirements. This security review will include completion of a security checklist ensuring that each of the security standards is implemented in accordance with the HMIS security plan.

III. Clark County HMIS Data Quality Plan

Training:
The System Administrator shall assure the provision of training of necessary participant staff in the use of ServicePoint. The System Administrator will provide training updates as necessary and reasonable due to staff changes and changes in technology.

Data Timeliness and Quality:
HMIS data is expected be entered within 5 working days following client contact.
Monthly HMIS data quality report cards will be provided to all participating agencies for the purpose of evaluating data quality and correcting errors/omissions. All HMIS participating agencies are expected to maintain a data report card grade of "A" (or over 95% completeness) for their programs. Programs who continually fail to meet their data quality expectations will be brought to the CoC steering Committee's attention for review and may be may subject to corrective action in the form of completing additional training, suspending or revoking specific user licenses or a participating program's HMIS system access as determined by the HMIS Lead Agency.
Overall system-wide data quality will be reported to all CoC members at the bi-monthly continuum of care coalition meeting.

Data User's Meetings:
Bi-monthly HMIS Data User Group meetings will be held for the purpose of addressing implementation and on-going operational issues. The User Group exists for the purpose of reviewing data quality, information sharing, problem-solving, and generating recommendations for the continued improvement of the local project and software upgrades. At least one representative from each HMIS participating agency is expected to attend.

COUNCIL FOR THE HOMELESS
Preventing and ending homelessness in Clark County

Attachment C

Homeless Management Information System (HMIS)

REMOTE ACCESS POLICY

The Agency Administrator and the System Administrator must approve remote access for a user. Since data entered into the data base requires a release of information signed by the client, it is important for all users to follow confidentiality policies covered in the Agency Participation Agreement and that client data pertinent to that client and agency only be accessed.

All remote access must be approved in writing and the ServicePoint Remote Access form (Attachment D) completed and signed by the Agency Administrator and the System Administrator.

The System Administrator will periodically audit all remote access. These audit reports show what clients were viewed, added, or edited by user.
These reports also show dates and times a client's file were accessed.

Violation of confidentiality policies can result in the termination of the Agency Participation Agreement.

Attachment D

Homeless Management Information System (HMIS)

ServicePoint Remote Access Agreement

The following user has been approved for remote access to the ServicePoint data base. The user will access only client data pertinent to that client for their agency. Remote access usage will be audited by the System Administrator.

User: _____

Agency: _____

Time Duration: _____

_____ _____

Agency Administrator Signature Date

_____ _____

System Administrator Signature Date

COUNCIL FOR THE HOMELESS
Preventing and ending homelessness in Clark County

Attachment E

USER AGREEMENT

AGENCY: _____

USER NAME: _____

Statement of Confidentiality*

Employees, volunteers, and any other persons with access to the Continuum of care Homeless Management Information System (HMIS) are subject to certain guidelines regarding the use of the HMIS. The HMIS contains a range of personal and private information on individuals. All such information must be treated carefully and professionally by all who access it.

Guidelines for use of the HMIS include:

- Personal User Identification and Passwords must be kept secure and not shared.
- Informed client or guardian consent, as documented by a **current** standard Release of Information (ROI) form, is required before entering, updating, editing, printing, or disclosing basic identifying information and non-confidential service transactions via the HMIS.
- Only general, non-confidential information is to be entered in the "other notes/comments" section of the Client Profile in the HMIS. Confidential information, including TB and HIV/AIDS diagnosis, domestic violence, and mental and/or physical health information, is not permitted to be entered in this section.
- Informed client or guardian consent, as documented by a **current** Agency-modified Release of Information form with a HMIS clause, is required before entering, updating, editing, printing, or disclosing information beyond basic identifying non-confidential information and service transactions.
- Confidential information obtained from the HMIS is to remain confidential, even if my relationship with _____ (agency name) changes or concludes for any reason.
- Information beyond basic identifying data, that includes all assessment screens (all screens beyond profile, agency, and community fields), is not to be edited. If an update or correction is needed, a new assessment must be created.
- Only individuals that exist as clients under the Agency's jurisdiction may be entered into the HMIS.
- Misrepresentation of the client base by entering known, inaccurate information is prohibited.
- Client records are not to be deleted from the HMIS. If a client or guardian of a client chooses to rescind consent to participate in the HMIS, her/his file shall become "inactive."
- Discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex, and sexual orientation are not permitted in the HMIS. Profanity and offensive language are not permitted in the HMIS.
- The HMIS is to be used for business purposes only. Transmission of material in violation of any United States Federal or State of Washington regulations or laws is prohibited and includes material that is copyrighted, legally judged to be threatening or obscene, and considered protected by trade secret. The HMIS will not be used to defraud the Federal, State, or local government or an individual entity or to conduct any illegal activity.
- Any unauthorized access or unauthorized modification to the HMIS computer system information or interference with normal system operations will result in immediate suspension of your access to the HMIS and may jeopardize your employment status with _____ (agency name).

Failure to comply with the provisions of this Confidentiality Statement is grounds for immediate termination. Your signature below indicates your agreement to comply with this statement of confidentiality. There is no expiration date of this agreement.

_____	_____	_____	_____
Signature	Date	Witness Signature, Title	Date
_____	_____	_____	_____
Printed Name	Date	Witness Printed Name	Date

*The original Statement of Confidentiality should be kept on file at the Agency. Forms on individuals no longer employed by the Agency should be kept on file for five years.