

Agency Partner Agreement

Washington State 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 Department of Commerce to collect HMIS data in the form of a data warehouse. Each homeless service provider will submit HMIS data to Commerce.

_____, (“Agency”) has elected to participate in HMIS.

Agency and the Department of Commerce 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 Commerce.
 - (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) “The Balance of State Continuum of Care Steering Committee” or “Steering Committee” refers to a Commerce advisory body that serves in a consultative and counseling capacity to Commerce as the system administrator. The Steering Committee is comprised of representatives from the State, the Balance of State Continuum of Care regions and at large members.
 - (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 information into HMIS, such information will be available to Commerce staff who may review the data to administer HMIS; to conduct analysis in partnership with the Research and Data Analysis (RDA) division at the Department of Social and Health Services (DSHS); and to prepare reports that may 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)**
 - (i) 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>
 - (ii) 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 Commerce 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** (or a Commerce-approved equivalent release document) 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 Commerce 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

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"), which is found on the Commerce web page (www.commerce.wa.gov/hmis) and is incorporated into this agreement and may be amended from time to time by Commerce. Agency will comply with, and enforce the User Policy and will inform Commerce 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-standards-final-notice/>) until the HMIS Proposed Rule is finalized and replaces the current Standards: <https://www.hudexchange.info/resource/1967/hearth-proposed-rule-for-hmis-requirements/>. 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 Commerce.
- 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 Commerce' HMIS; the end-user is expected to physically enter the password each time he or she logs on to the system

- 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 Commerce.

- e. **Training/Assistance:** Agency will permit access to HMIS only after the authorized user receives appropriate confidentiality training including that provided by Commerce. 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 Commerce. Commerce will be reasonably available during Commerce defined weekday business hours for technical assistance (i.e. troubleshooting and report generation).
- f. **Records:** Agency and Commerce 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 Commerce will provide an accounting of all such disclosures within the prior **seven**-year period. Commerce 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.

- 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 Commerce 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. Steering Committee: Commerce will consult with the Steering Committee from time to time regarding issues such as revision to the form of this Agreement. Written Agency complaints that are not resolved may be forwarded to the Steering Committee, which will try to reach a voluntary resolution of the complaint.

12. 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

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.

13. Limitation of Liability. Commerce 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.

14. Disclaimer of Warranties. Commerce 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.

15. Additional Terms and Conditions:

- a. Agency will abide by such guidelines as are promulgated by HUD and/or Commerce from time to time regarding administration of the HMIS.
- b. Agency and Commerce 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 Commerce agree to modify the terms of this agreement so as to comply with applicable law.
- c. Neither Commerce 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 Commerce 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 Commerce Security Policy by Agency.
- f. If this Agreement is terminated, Agency will no longer have access to HMIS. Commerce 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,

_____ Executive Director Signature	_____ Print Executive Director Name	_____ Date	
_____ Agency Name			
_____ Street Address	_____ City	_____ State	_____ Zip Code
_____ Mailing Address <i>(Leave Blank If Same As Above)</i>	_____ City	_____ State	_____ Zip Code
_____ Diane Klontz, Assistant Director Community Services and Housing Division		_____ Date	