Department of Commerce

Guidelines

FOR THE

Consolidated Homeless Grant
System Demonstration Grant

July 1, 2019 – June 30, 2021
# Table of Contents

1 Introduction .................................................................................................................. 6  
   1.1 Overview ................................................................................................................. 6  
   1.2 Authorizing Statute and Fund Sources ................................................................. 6  

2 Administrative Requirements ........................................................................................... 7  
   2.1 Prioritize Unsheltered Homeless Households ....................................................... 7  
   2.2 Homeless System Performance Requirements .................................................. 7  
   2.3 Low Barrier Housing Project .............................................................................. 7  
   2.4 Coordinated Entry ............................................................................................... 8  
   2.5 HMIS .................................................................................................................... 8  
      2.5.1 Data Timeliness .............................................................................................. 8  
      2.5.2 Data Quality .................................................................................................. 9  
      2.5.3 Consent for Entry of Personally Identifying Information ......................... 9  
   2.6 Reporting Requirements ....................................................................................... 10  
      2.6.1 Local Homeless Housing Plan .................................................................... 10  
      2.6.2 Annual County Expenditure Report ............................................................ 10  
      2.6.3 Point-in-Time Count .................................................................................... 10  
      2.6.4 Essential Needs Report ................................................................................ 11  
   2.7 Training .................................................................................................................. 11  
   2.8 Benefit Verification System Requirements .......................................................... 11  
   2.9 Interested Landlord List ....................................................................................... 12  
   2.10 Outreach to Landlords ....................................................................................... 12  
   2.11 Grant Management ............................................................................................. 12  
      2.11.1 Changes to Guidelines ................................................................................ 12  
      2.11.2 Commerce Monitoring ............................................................................. 12  
      2.11.3 Subgrantee Requirements ......................................................................... 12  

3 Fiscal Administration .................................................................................................... 13  
   3.1 Ineligible Use of Funds ...................................................................................... 13  
   3.2 Budget Caps ......................................................................................................... 13  
   3.3 Reimbursements .................................................................................................... 14  
      3.3.1 Back-up Documentation ............................................................................. 14  
   3.4 Budget Revisions .................................................................................................. 14
1 Introduction

1.1 Overview

The Consolidated Homeless Grant (CHG) provides resources to fund homeless crisis response systems to support communities in ending homelessness. Homeless crisis response systems respond to the immediacy and urgency of homelessness and make sure that everyone has a safe and appropriate place to live. The vision, principles and goals set forth in the State Homeless Strategic Plan guide the management and implementation of CHG.

The State Homeless Housing Strategic Plan and Annual Report of the Homeless Grant Programs are located on the Department of Commerce website.

1.2 Authorizing Statute and Fund Sources

Chapter RCW 43.185c Homeless Housing and Assistance authorizes these funds.
2 Administrative Requirements

2.1 Prioritize Unsheltered Homeless Households

Grantees must prioritize unsheltered homeless households for services and projects.

For more details, see Appendix A: Performance Requirements.

2.2 Homeless System Performance Requirements

Grantees must maintain performance measures to help evaluate their effectiveness as they work to ensure that homelessness is rare, brief, and one time.

For more details, see Appendix A: Performance Requirements.

2.3 Low Barrier Housing Project

Each county must have at least one low barrier project\(^1\) serving homeless adults and at least one low barrier project serving homeless households with children.

All homeless housing projects adhere to state and federal anti-discrimination laws:

- All projects ensure equal access for people experiencing homelessness regardless of race, national origin, gender identity, sexual orientation, marital status, age, veteran or military status, disability, or the use of an assistance animal.
- Projects designed to serve families with children experiencing homelessness ensure equal access regardless of family composition and regardless of the age of a minor child.
- Projects that operate gender segregated facilities allow the use of facilities consistent with the person’s gender expression or identity.

2.3.1 Intake & Project Eligibility

Low barrier projects have flexible intake schedules and require minimal documentation. At the minimum, homeless households are not screened out based on the following criteria:

- Having too little or no income
- Having poor credit or financial history
- Having poor or lack of rental history
- Having involvement with the criminal justice system
- Having active or a history of alcohol and/or substance use
- Having a history of victimization

\(^1\) Project types that can meet this requirement: Emergency Shelter, Transitional Housing, PH: Rapid Re-Housing, PH: Housing with Services (no disability requirement), and PH: Housing Only. Projects that operate seasonally do not meet this requirement.
The type or extent of disability-related services or supports that are needed
Lacking ID or proof of U.S. Residency Status
Other behaviors that are perceived as indicating a lack of “housing readiness,”
including resistance to receiving services

2.3.1.2 Project Participation
Low barrier projects have realistic and clear expectations. Rules and policies are
narrowly focused on maintaining a safe environment and avoiding exits to
homelessness. Low barrier projects do not have work or volunteer requirements.
Projects that require people to pay a share of rent allow reasonable flexibility in
payment.

Households are not terminated from the project for the following reasons:
- Failure to participate in supportive services or treatment programs
- Failure to make progress on a housing stability plan
- Alcohol and/or substance use in and of itself is not considered a reason for
termination

2.4 Coordinated Entry
Each county must maintain a coordinated entry system (CES). Refer to the Washington State
Coordinated Entry Guidelines for requirements.

2.5 HMIS
Grantees must require client data to be entered into the Homeless Management
Information System (HMIS) for all temporary and permanent housing interventions
regardless of funding source.

Additionally all Emergency Shelter, Transitional Housing, Safe Haven, Homelessness
Prevention or any Permanent Housing\(^2\) type program funded with local document
recording fees must enter client data in HMIS.

2.5.1 Data Timeliness
Grantees must require client data to be entered into HMIS no later than the 20th
calendar day following the end of each month.

Counties not using the State HMIS (data integration counties), must upload data to the
State’s HMIS data warehouse using XML or CSV schema compliant with current HUD
HMIS Data Standards. Uploads must occur no later than the 30th calendar day following
the end of each month. Counties not able to export and upload client data to the state
HMIS must use the state HMIS for client data entry.

\(^2\) PH – Permanent Supportive Housing, PH – Housing Only, PH – Housing with Services, PH – Rapid Re-Housing
2.5.2 Data Quality
Grantees must develop data quality expectations for subgrantees. Data quality is measured by the percent of valid data collected for each data element. “Client doesn’t know”, “Client refused”, and “Data not collected” are considered invalid responses.

Commerce will annually score county HMIS data quality. This score will be reported on the Homeless System Performance County Report Card.

2.5.3 Consent for Entry of Personally Identifying Information

2.5.3.1 Identified Records
✓ Personally identifying information (PII)\(^3\) must not be entered into HMIS unless all adult household members have provided informed consent.
✓ Informed consent must be documented with a signed copy of the Client Release of Information and Informed Consent Form in the client file. If electronic consent has been received, a copy does not need to be printed for the client file but must be available in HMIS. If telephonic consent has been received, complete the consent form the first time the household is seen in person.

2.5.3.2 Anonymous Records
The following types of records must be entered anonymously:
✓ Households in which one or more adult member does not provide informed consent for themselves or their dependents
✓ Households entering a domestic violence program or currently fleeing violence (domestic violence, dating violence, sexual assault, trafficking, stalking or other life threatening situation)
✓ Minors under the age of 13 with no parent or guardian available to consent to the minor’s information in HMIS
✓ Households in programs that are required by funders to report HIV/AIDS status

2.5.3.3 Special Circumstances
If the reporting of the HIV/AIDS status of clients is not specifically required, the HIV/AIDS status must not be entered in HMIS.

If a combination of race, ethnicity, gender, or other demographic data could be identifying in your community, those data should not be entered for anonymous records.

2.5.3.4 Records Maintenance and Destruction
Paper records derived from HMIS, which contain personally identifying information, must be destroyed within seven years after the last day the household received services from the lead/subgrantee.

---

\(^3\) PII includes name, social security number, birthdate, address, phone number, email, and photo.
2.6 Reporting Requirements

2.6.1 Local Homeless Housing Plan

Lead grantees must submit an updated county Local Homeless Housing Plan to Commerce at least every five years. Local plans must include performance goals and strategies. Performance in meeting the goals of the local plan should be assessed annually. Information from the Annual Homeless Housing County Inventory and Expenditure Report and the Annual Point in Time Count should help inform the local plan.

At a minimum, local plans should:

- Connect the needs of people experiencing homelessness, the current and future housing inventory, available resources, and community goals and priorities.
- Describe system and/or program inventory (both housing and services only) changes and its quantitative impact on reducing homelessness. Describe the costs of the associated with these changes.
- Describe implementation dates and names of responsible parties.

Participants involved in development of local plans should include representation of a person who has experienced homelessness, and all homeless housing providers including emergency shelters, outreach teams, transitional and permanent supportive housing agencies. Behavioral health and chemical dependency service providers, school liaisons and local jail administrators should also be included. Counties are encouraged to engage local DSHS community service offices, community colleges, public health, and local employment partners.

2.6.2 Annual County Expenditure Report

Grantees must submit an Annual County Expenditure Report to Commerce.

Commerce will annually score a lead grantees Annual County Expenditure Report data quality. This score will be reported on the Homeless System Performance County Report Card.

Grantees should work to increase their Annual County Expenditure Report data quality. Beginning July 2019, grantees must increase their data quality from their 2018 Report Card baseline.

2.6.3 Point-in-Time Count

Grantees must ensure the collection and reporting of the annual Point-in-Time Count of sheltered and unsheltered homeless persons for their county in accordance with the Commerce Count Guidelines, which are posted at http://www.commerce.wa.gov/serving-communities/homelessness/annual-point-time-count/.
2.6.4 Essential Needs Report

Grantees must submit an HEN Essential Needs Report at the end of each state fiscal year, which is a count of the total instances of Essential Needs services.

2.7 Training

Lead/subgrantee staff that provide direct services and supervise staff who provide direct services and manage homeless grants should receive training and demonstrate competency in, at a minimum:

✓ Trauma Informed Services
✓ Mental Health First Aid
✓ Harm Reduction
✓ Supporting victims of domestic violence
✓ Local coordinated entry policies and procedures
✓ Fair Housing

In addition, Lead/subgrantee staff are highly encouraged to attend the annual Washington State Conference on Ending Homelessness.

Costs to attend trainings are an eligible program expense (see Section 6.3 Operations).

2.8 Benefit Verification System Requirements

Commerce maintains a data share agreement with the Department of Social and Health Services (DSHS) so homeless housing grantees can access the Benefits Verification System (BVS) to confirm Housing and Essential Needs and Temporary Assistance to Needy Families program eligibility. The BVS can also be used to confirm benefits and financial eligibility for homeless housing programs.

Lead grantees manage BVS User access for their staff and sub grantees. Upon approval by Commerce, lead grantees can also appoint another agency as the BVS lead for their county.

BVS leads are responsible for the following:

✓ Review User requests to confirm requesting agency is a sub grantee and staff have a business need to access the BVS system.
✓ Confirm that each User request includes a signed DSHS Non-Disclosure form.
✓ Retain all signed DSHS Non-Disclosure forms.
✓ Maintain an Excel spreadsheet identifying current and past BVS Users. Spreadsheet must be in format designated by Commerce.
✓ Report to Commerce within one business day when User no longer require access to BVS.
✓ Provide access to DSHS Non-Disclosure forms and User spreadsheet for inspection within one business day of request by Commerce or DSHS.
BVS Leads are also responsible for the following, **annually:**
- ✓ Require users to re-sign DSHS Non-Disclosure form.
- ✓ Review BVS User spreadsheet for accuracy and notify Commerce of any changes.
- ✓ Notify Commerce via email upon completion of annual requirements.

See Appendix C: Access to the DSHS Benefits Verification System for additional details.

<table>
<thead>
<tr>
<th>2.9 Interesting Landlord List</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Grantees are responsible for ensuring that an interested landlord list is created and maintained. The interested landlord list must include information on rental properties (including buildings with fewer than 50 units.) The list must be updated at least once per quarter, and distributed to partner agencies and households offered rent assistance. See RCW 43.185c.240. Creation and maintenance of the list may be delegated to another entity.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.10 Outreach to Landlords</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Grantees are responsible for ensuring that outreach to private rental housing landlords is conducted and documented at least quarterly. Outreach to private landlords includes information about opportunities to provide rental housing to people experiencing homelessness. See RCW 43.185c.240. Outreach and documentation may be delegated to another entity.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.11 Grant Management</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2.11.1 Changes to Guidelines</td>
<td>Commerce may revise the guidelines at any time. All Grantees will be sent revised copies.</td>
</tr>
<tr>
<td>2.11.2 Commerce Monitoring</td>
<td>Commerce will monitor grantee CHG grant activities. Grantees will be given a minimum of 30 days’ notice unless there are special circumstances that require immediate attention. The notice will specify the monitoring components.</td>
</tr>
<tr>
<td>2.11.3 Subgrantee Requirements</td>
<td>The CHG Grant General Terms &amp; Conditions Section 32 identifies subgrantee requirements. In addition, all subgrantee agreements must be time-limited and have defined roles and responsibilities for each party, detailed budgets and performance terms. Commerce reserves the right to directly contact subgrantees at any time for data quality, monitoring, fiscal and other issues.</td>
</tr>
</tbody>
</table>

Grantees may enter into an agreement with any other local government, Council of Governments, Housing Authority, Community Action Agency, Regional Support Network (under 71.24 RCW), nonprofit community or neighborhood-based organization, federally recognized Indian tribe in the state of Washington, or regional or statewide nonprofit housing assistance organizations who operate programs to end homelessness within a defined service area.
Grantees must provide Commerce with copies of subgrant agreements (upon request) and notify Commerce if subgrantee agreements are terminated during the grant period.

Grantees must notify Commerce of any changes in selection of subgrantees funded with CHG, or changes in the interventions of those subgrantees.

2.11.3.1 Subgrantee Risk Assessment and Monitoring
Grantees are responsible for ensuring subgrantee compliance with all requirements identified in the CHG guidelines. The Grantee must conduct a risk assessment and develop a monitoring plan for each subgrantee within six months of contracting CHG funds to the subgrantee. The risk assessment must inform the monitoring plan for each subgrantee. Monitoring plans must include monitoring dates, the type of monitoring (remote, on-site), and the program requirements being reviewed.

Grantees must maintain policies and procedures that guide the risk assessment, monitoring activities, and monitoring frequency.

Commerce reserves the right to require grantees to undertake special reviews when an audit or other emerging issue demands prompt intervention and/or investigation.

2.11.3.2 Subgrantee Performance Measure Requirements
Locally developed performance measures with applicable targets or benchmarks must be included in subgrantee agreements.

For more details, see Appendix A: Performance Requirements.

3 Fiscal Administration

3.1 Ineligible Use of Funds
Grantees must inform Commerce if CHG funds are spent on ineligible households or expenses. Reasonable attempts must be made to prevent fraud and ensure allowable use of funds.

3.2 Budget Caps
✓ For-Profit Set Aside - At least 36 percent of the non-HEN CHG funds must be budgeted and spent on rent/lease payments to for-profit and non-profit entities, including housing authorities.
✓ Administration - up to 15 percent of total non-HEN reimbursed costs may be used for administration.
✓ HEN Administration - up to 7 percent of total HEN reimbursed costs may be used for HEN administration.
✓ Temporary Assistance for Needy Families (TANF) households - the sum of TANF
household budget categories must always be equal to the original TANF household allocation.

- HEN Households - the sum of HEN household budget categories must always be equal to the original HEN household allocation.

### 3.3 Reimbursements

Grantees must bill Commerce monthly for reimbursement of allowable costs. Invoices are due on the 20th of the month following the provision of services. Final invoices for a biennium may be due sooner than the 20th. If the grantee fails to submit an invoice within a three-month period, without a reasonable explanation, Commerce may take corrective action as outlined in the CHG grant Scope of Work. Exceptions to billing procedures can be negotiated with Commerce on a case-by-case basis.

Invoices must be submitted online using the Commerce Contract Management System (CMS) through Secure Access Washington (SAW).

#### 3.3.1 Back-up Documentation

All submitted invoices must include the CHG Voucher Detail and any required HMIS reports. Invoices may not be paid until the report(s) are received and verified. Commerce may require a grantee to submit additional documentation. Grantee must retain original invoices submitted by their subgrantees.

### 3.4 Budget Revisions

Revisions must be submitted using the Budget Revision Tool and approved by Commerce. Budget Caps must be maintained with each revision. A contract amendment is required when revisions (in one or cumulative transfers) reach more than 10 percent of the grant total.
4 Allowable Interventions

4.1 Temporary Housing Interventions
Temporary housing interventions are those in which the household must leave the shelter or unit at the end of their program participation. Households are considered homeless while enrolled in temporary housing interventions.

4.1.1 Emergency Shelter
Emergency shelter provides short-term emergency shelter (lodging) for those experiencing homelessness. Emergency Shelters can be facility-based, or hotel/motel voucher.

4.1.1.1 Drop-in Shelter
Drop-in Shelters offer night-by-night living arrangements that allow households to enter and exit on an irregular or daily basis.

4.1.1.2 Continuous-stay Shelter
Continuous-stay Shelters offer living arrangements where households have a room or bed assigned to them throughout the duration of their stay.

4.1.2 Transitional Housing
Transitional housing is subsidized, facility-based housing that is designed to provide long-term temporary housing and to move households experiencing homelessness into permanent housing. Lease or rental agreements are required between the transitional housing project and the household.

4.2 Permanent Housing Interventions
Permanent housing is housing in which the household may stay as long as they meet the basic obligations of tenancy.

4.2.1 Targeted Prevention
Targeted Prevention resolves imminent homelessness with housing-focused case management and temporary rent subsidies.

4.2.2 Rapid Re-Housing
Rapid Re-Housing (RRH) quickly moves households from homelessness into permanent housing by providing move in assistance, temporary rent subsidies, and housing-focused case management. The household does not have to leave the unit when assistance ends.

4 Allowable Interventions

4.1 Temporary Housing Interventions
Temporary housing interventions are those in which the household must leave the shelter or unit at the end of their program participation. Households are considered homeless while enrolled in temporary housing interventions.

4.1.1 Emergency Shelter
Emergency shelter provides short-term emergency shelter (lodging) for those experiencing homelessness. Emergency Shelters can be facility-based, or hotel/motel voucher.

4.1.1.1 Drop-in Shelter
Drop-in Shelters offer night-by-night living arrangements that allow households to enter and exit on an irregular or daily basis.

4.1.1.2 Continuous-stay Shelter
Continuous-stay Shelters offer living arrangements where households have a room or bed assigned to them throughout the duration of their stay.

4.1.2 Transitional Housing
Transitional housing is subsidized, facility-based housing that is designed to provide long-term temporary housing and to move households experiencing homelessness into permanent housing. Lease or rental agreements are required between the transitional housing project and the household.

4.2 Permanent Housing Interventions
Permanent housing is housing in which the household may stay as long as they meet the basic obligations of tenancy.

4.2.1 Targeted Prevention
Targeted Prevention resolves imminent homelessness with housing-focused case management and temporary rent subsidies.

4.2.2 Rapid Re-Housing
Rapid Re-Housing (RRH) quickly moves households from homelessness into permanent housing by providing move in assistance, temporary rent subsidies, and housing-focused case management. The household does not have to leave the unit when assistance ends.

---

4 Emergency Shelter programs are typically designed and intended to provide temporary shelter for short-term stays: up to three months. Clients are not required to exit after 90 days.

5 Transitional Housing programs are typically designed and intended to provide temporary housing for long-term stays: up to two years.
### 4.2.3 Permanent Supportive Housing

Permanent Supportive Housing (PSH) is subsidized, non-time-limited housing with support services for homeless households that include a household member with a permanent disability. Support services must be made available but participation is voluntary. PSH may be provided as a rent assistance (scattered site) or facility-based model. For facility-based model, a lease or rental agreement is required between the PSH project and the household. The services and the housing are available permanently.

### 4.3 Services Only Interventions

#### 4.3.1 Outreach

Street outreach is a strategy for engaging people experiencing homelessness who are otherwise not accessing services for the purpose of connecting them with emergency shelter, housing, or other critical services.
5 Household Eligibility

A household is one or more individuals seeking to obtain or maintain housing together. The entire household is considered for eligibility determination and services. A household does not include friends or family that is providing temporary housing.

Eligible households must meet both housing status and income requirements as detailed in the following sections.

<table>
<thead>
<tr>
<th>Housing Status</th>
<th>Income</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homeless</td>
<td>At or below 30% area median income</td>
</tr>
<tr>
<td>OR</td>
<td>OR</td>
</tr>
<tr>
<td>At imminent risk of</td>
<td>HEN Referral, General Assistance</td>
</tr>
<tr>
<td>homelessness</td>
<td>enrolled (ABD recipient)</td>
</tr>
<tr>
<td></td>
<td>OR</td>
</tr>
<tr>
<td></td>
<td>TANF enrolled</td>
</tr>
</tbody>
</table>

5.1 Housing Status Eligibility

5.1.1 Homeless

Households are homeless if they are unsheltered or residing in a temporary housing program, as defined below.

5.1.1.1 Unsheltered Homeless:

✓ Living outside or in a place that is not designed for, or ordinarily used as a regular sleeping accommodation for human beings, including a vehicle, park, abandoned building, bus or train station, airport, or campground

✓ Fleeing or attempting to flee violence: domestic violence, dating violence, sexual assault, stalking, human trafficking, or other dangerous or life-threatening conditions that relate to violence against the household member(s), including children, that have either taken place within the household’s primary nighttime residence or has made the household member(s) afraid to return to their primary nighttime residence

5.1.2 Sheltered Homeless:

✓ Residing in a temporary housing program including shelters, transitional or interim housing, and hotels and motels paid for by charitable organizations or
government programs
- Exiting a system of care or institution where they resided for 90 days or less AND who resided in an emergency shelter or place not meant for human habitation immediately before entering that system of care or institution
- Residing in a trailer or recreational vehicle that is parked illegally or in a location that is not intended for long-term stays (i.e. parking lots)

### 5.1.2 At Imminent Risk of Homelessness
Households are at imminent risk of homelessness if they will lose their primary nighttime residence (including systems of care or institutions) within 14 days of the date of application for assistance, AND no subsequent residence has been identified, AND the household lacks the resources or support networks needed to obtain other permanent housing.

### 5.2 Documentation of Housing Status
An eligible Housing Status must be verified and documented prior to program entry.

Households entering emergency shelter are exempt from housing status requirements.

### 5.3 Income Eligibility
The combined household income must not exceed 30 percent of area median income as defined by HUD. Income limits are based on Area Median Income (AMI), which can be located for each county at: [www.huduser.gov](http://www.huduser.gov) (Data Sets, Income Limits).

#### 5.3.1 Income Eligibility Exemptions
Income eligibility requirements are never required for Drop-in Shelter or for households receiving only Flex Funding.

The following are exempt from income eligibility requirements for the first 90 days of program participation:
- Households entering Transitional Housing
- Households entering a Rapid Re-Housing program
- Households entering a Continuous-stay Shelter

**Assistance for HEN households:** In place of income verification, a HEN Referral or General Assistance enrollment (ABD recipient) from the Washington State Department of Social and Health Services (DSHS) as documented in the Benefits Verification System (BVS) is required.

**Assistance for TANF households:** In place of income verification, proof of TANF Enrollment from DSHS is required.
<table>
<thead>
<tr>
<th>Temporary Housing Interventions</th>
<th>Enrollment</th>
<th>Recertification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drop-in Shelter</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>Continuous-stay Shelter</td>
<td>None</td>
<td>At or below 30% AMI</td>
</tr>
<tr>
<td>Transitional Housing</td>
<td>None</td>
<td>At or below 30% AMI</td>
</tr>
<tr>
<td>Permanent Housing Interventions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHG Rapid Re-Housing</td>
<td>None</td>
<td>At or below 30% AMI</td>
</tr>
<tr>
<td>CHG Targeted Prevention</td>
<td>At or below 30% AMI</td>
<td>At or below 30% AMI</td>
</tr>
<tr>
<td>TANF Rapid Re-Housing and Targeted Prevention</td>
<td>TANF Enrollment</td>
<td>TANF Enrollment</td>
</tr>
<tr>
<td>HEN Rapid Re-Housing and Targeted Prevention</td>
<td>DSHS HEN Referral or General Assistance enrolled (ABD recipient)</td>
<td>DSHS HEN Referral or General Assistance enrolled (ABD recipient)</td>
</tr>
<tr>
<td>Permanent Supportive Housing</td>
<td>At or below 30% AMI and a household member with a permanent disability</td>
<td>None</td>
</tr>
</tbody>
</table>
5.4 Documentation of Income Eligibility
Income Eligibility must be verified and documented prior to program entry.

5.4.1 Documentation of HEN Referral, General Assistance Enrollment (ABD Recipient) or TANF Enrollment
HEN Referral, General Assistance enrollment (ABD recipient) or TANF Enrollment must be verified and documented prior to program entry.

**Assistance for HEN households**: the HEN Referral or General Assistance enrollment (ABD recipient) from the Washington State Department of Social and Health Services (DSHS) as documented in the Benefits Verification System (BVS) is required and must be kept in the client file.

**Assistance for TANF households**: proof of TANF enrollment from DSHS is required and must be kept in the client file.

5.5 Eligibility Recertification
Income eligibility must be documented at least every three months.

**Assistance for HEN households**: Recertification of the HEN Referral or General Assistance enrollment (ABD recipient) from DSHS as documented in the Benefits Verification System (BVS) is required at least every three months.

**Assistance for TANF households**: Recertification of TANF enrollment from DSHS is required at least every three months.

5.5.1 Income Ineligible at Recertification
If households are determined income ineligible, they may remain in the program for an additional three months. Case management may continue for an additional six months after the determination of income ineligibility to support the household transition to self-sufficiency.

If the household is no longer eligible for the HEN program, the three additional months of rent assistance **may not** be charged to HEN but may be charged to the CHG base funding.

If the household is no longer enrolled in TANF, the three additional months of rent assistance **may** be charged to the TANF budget or the CHG base funding.

5.6 Additional Eligibility Requirements for Permanent Supportive Housing
To be eligible for permanent supportive housing, a household must be homeless AND include at least one household member who has a disability that is expected to be long continuing or of indefinite duration and substantially impedes the household member’s ability to live independently.
Disability includes: a physical, developmental, mental, or emotional impairment, including impairment caused by alcohol or drug abuse, post-traumatic stress disorder, or brain injury. A person will also be considered to have a disability if he or she has Acquired Immune Deficiency Syndrome (AIDS) or any conditions arising from the etiologic agent for 86 Acquired Immune Deficiency Syndrome, including infection with the Human Immunodeficiency Virus (HIV).

### 5.6.1 Documentation of a Disability

Disability must be verified and documented prior to program entry. Acceptable documentation of the disability must include one the following:

- Written verification of the disability from a professional licensed by the state to diagnose and treat the disability and his or her certification that the disability is expected to be long continuing or of indefinite duration and substantially impedes the individual’s ability to live independently
- Written verification from the Social Security Administration
- Disability check receipt (Social Security Disability Insurance check or Veteran Disability Compensation)
- Other documentation approved by Commerce

If unable to document disability at program entry with the above methods, program staff must record observation of disability. Required documentation (above) must be obtained within 45 days of program enrollment.

### 5.6.2 Maintaining Homeless Status for Permanent Housing

While receiving Rapid Re-Housing assistance, households maintain their homeless status for purposes of eligibility for other permanent housing placements.
6 Allowable Expenses

6.1 Rent

Rent Payments and Other Housing Costs must be paid directly to a third party on behalf of the household.

6.1.1 Rent Payments

- Monthly rent and any combination of first and last months’ rent. Rent assistance is not time-limited
- Rental arrears and associated late fees. Rental arrears for HEN or TANF enrolled clients can be paid for a time when the client was not HEN or TANF enrolled.
- Lot rent for RV or manufactured home
- Costs of parking spaces when connected to a unit
- Landlord incentives, including reimbursement for damages paid to a landlord
- Security deposits for households moving into new units
- Hotel/Motel expenses are allowable when used as permanent housing or when used as Emergency Shelter when a suitable shelter bed is not available.
- Utilities that are included in rent
- Other fees that are included in rent

6.1.2 Other Housing Costs

- Utility payments
- Utility arrears
- Utility deposits for a household moving into a new unit
- Application fees, background, credit check fees, and costs of urinalyses for drug testing of household members if necessary/required for rental housing
- Other costs as approved by Commerce

6.1.3 Special Circumstances

- Master-lease: Security deposit and monthly rent is allowable when an organization master-leases a unit, and then sub-leases the property to CHG eligible households in the context of a Rapid Re-Housing or Permanent Supportive Housing program.
- Temporary absence: If a household must be temporarily away from the unit, but is expected to return grantees may pay for the household’s rent for up to 60 days.
- Subsidized housing: CHG rent/utility assistance may be used for move-in costs (security deposits, first and last month’s rent) for subsidized housing (where household’s rent is adjusted based on income), including project- or tenant-based housing. CHG may also be used for rental arrears or utility arrears for subsidized housing.

---

6 In this context tax credit units are not considered subsidized housing.
6.1.4 Ineligible Expenses

- Ongoing rent/utilities for subsidized housing
- CHG rent and rent/utility assistance in combination with CHG-funded facility support
- Cable deposits or services
- Mortgage assistance and utility assistance for homeowners

6.2 Facility Support

6.2.1 Lease Payments

- Lease or rent payment on a building used to provide temporary housing or permanent supportive housing
- Hotel/Motel expenses for less than 90 days when no suitable shelter bed is available
- Move-in costs (security deposits, first and last month’s rent) for permanent housing

6.2.2 Other Facility Costs

- Utilities
- Facility Maintenance supplies and services. Maintenance activities include cleaning activities; protective or preventative measures to keep a building, its systems, and its grounds in working order; and replacement of existing appliances or objects that are not fixtures or part of the building.
- Security and janitorial services
- Essential facility equipment and supplies
- Expendable transportation costs
- On-site and off-site management costs related to the building
- Facility specific insurance (mortgage insurance is not allowable) and accounting
- Costs for securing permanent housing including: application fees, background check fees, credit check fees, utility deposits, and costs of urinalyses for drug testing of household members if necessary/required for housing
- Other expenses as approved by Commerce

6.2.3 Ineligible Expenses

- Replacement or operating reserves
- Debt service
- Construction or rehabilitation of shelter facilities
- CHG facility support in combination with CHG funded rent and rent/utility assistance
- Mortgage payment for the facility

---

7For reimbursements, this includes lease payments made to government and tribal governments.
**6.2.4 HEN and TANF Facility Support**

HEN and TANF facility support must be proportionally billed according to an estimate of the number of HEN or TANF households expected to occupy the facility.

For HEN funding, lease payments and other facility costs are allowable for transitional and permanent supportive housing, but not for emergency shelter.

**6.3 Operations**

Operations expenses are directly attributable to a particular program or to the homeless crisis response system.

- Salaries and benefits for staff costs directly attributable to the program or to the homeless system, including but not limited to program staff, information technology (IT) staff, human resources (HR) staff, bookkeeping staff, and accounting staff
- Office space, utilities, supplies, phone, internet, and training related to grant management and/or service delivery/conferences/travel and per diem
- Equipment up to $1,500 per grant period unless approved in advance by Commerce

**6.3.1 Homeless Crisis Response System Expenses**

- Point-in-Time counts
- Annual report/housing inventory
- Local homeless plans
- Coordinated entry planning, implementation and operations
- State data warehouse and Homeless Management Information System
- Interested landlord list and landlord outreach activities
- Participation in local Continuum of Care

**6.3.2 Program Expenses**

- Intake and Assessment
- Housing Stability Services
- Housing Search and Placement Services
- Outreach services
- Optional support services
- Mediation and outreach to property owners (landlord incentives)
- Data collection and entry
- General liability insurance and automobile insurance
- Other costs as approved in advance by Commerce

**6.3.3 Flexible Funding**

Flexible Funding is the provision of goods or payments of expenses not included in other allowable expense categories, which directly help a household to obtain or maintain permanent housing or meet essential household needs. Essential household needs means personal health and hygiene items, cleaning supplies, transportation passes and other personal need items (WAC 388-400-0065).
Households are eligible for Flexible Funding up to $1,500 per household. Essential household need items are exempt from the $1,500 cap, and are available to households with a HEN referral, or who are otherwise eligible for CHG.

Flexible Funding payments must be paid directly to a third party on behalf of the household.

### 6.3.4 Ineligible Expenses

- Retailer or merchant gift cards, vouchers, or certificates that can be exchanged for cash or that allow the recipient to purchase alcohol or tobacco products

### 6.4 Administration

Up to 15 percent of total non-HEN reimbursed costs and up to 7 percent of total HEN reimbursed costs over the course of the grant period may be used for administration. This limit must be reconciled before the end of the grant period.

Allowable administrative costs benefit the organization as a whole and cannot be attributed specifically to a particular program or to the homeless crisis response system. Administrative costs may include the same types of expenses that are listed in program operations (such as IT staff and office supplies), in the case that these costs are benefiting the agency as a whole and are not attributed to a particular program or the homeless system. Administrative costs may include, but are not limited to, the following:

- Executive director salary and benefits
- General organization insurance
- Organization wide audits
- Board expenses
- Organization-wide membership fees and dues
- Washington State Quality Award (WSQA) expenses
- General agency facilities costs (including those associated with executive positions) such as rent, depreciation expenses, and operations and maintenance

All amounts billed to administration must be supported by actual costs. If actual costs exceed the budgeted limit, they may be charged in equal monthly amounts. These costs must be charged to grant cost centers by one of the following three methods:

- Billed directly such as IT services that are billed by the hour.
- Shared costs that are allocated directly by means of a cost allocation plan.
- Costs related to executive personnel such that a direct relationship between the cost and the benefit cannot be established must be charged indirectly by use of an indirect cost rate which has been appropriately negotiated with an approved cognizant agency or by use of the 10 percent de minimus rate.
7 Requirements of Direct Service Programs

7.1 Ensure Habitability

Documented habitability is required for all housing units into which households will be moving, except when a household moves in with friends or family or into a hotel/motel unit.

Housing units must be documented as habitable prior to paying the rent subsidy. Allowable methods for unit habitability determination include landlord certification of habitability or a unit inspection.

All facilities must conduct and document an inspection at least once a year.

7.1.1 Habitability Complaint Procedure

Each household must be informed in writing of the habitability complaint process and assured that complaints regarding their housing unit’s safety and habitability will not affect the household’s program eligibility.

Lead/subgrantee must have a written procedure describing the response to complaints regarding unit safety and habitability. The procedure must include mandatory inspection when a complaint is reported using the HHS Form, HQS Inspection Form, or documenting the specific complaint in an alternate format that includes follow-up and resolution.

7.2 Lead Based Paint Assessment

To prevent lead poisoning in young children, programs must comply with the Lead-Based Paint Poisoning Prevention Act of 1973 and its applicable regulations found at 24 CFR 35, Parts A, B, M, and R.

For a guide to compliance see Appendix B: Lead Based Paint Visual Assessment Requirements.

7.2.1 For Rent Assistance

A lead-based paint visual assessment must be completed prior to providing rapid re-housing, prevention rent assistance if a child under the age of six, or pregnant woman resides in a unit constructed prior to 1978.

7.2.2 For Facilities

All facilities that may serve a child under the age of six or a pregnant woman constructed prior to 1978 must conduct and document an annual lead-based paint visual assessment.
7.2.3 **Exceptions to the Lead-Based Paint Visual Assessment Requirement**

Visual assessments are not required under the following circumstances:

- Zero-bedroom or SRO-sized units;
- X-ray or laboratory testing of all painted surfaces by certified personnel has been conducted in accordance with HUD regulations and the unit is officially certified to not contain lead-based paint;
- The property has had all lead-based paint identified and removed in accordance with HUD regulations;
- The unit has already undergone a visual assessment within the past 12 months – obtained documentation that a visual assessment has been conducted; or
- It meets any of the other exemptions described in 24 CFR Part 35.115(a).

7.3 **Informed Consent to Review Information in the Benefits Verification System**

Programs may review confidential information in the BVS only after all adult household members have provided informed consent as documented using the form *DSHS 14-012(x)(REV 02/2003)*. See Appendix C: Benefits Verification System Data Security Requirements for more information.

7.4 **Personal Identifying Information**

Personal identifying information must never be sent electronically unless sent via a secure file transfer. Request secure file transfer login credentials from Commerce.

7.5 **Prohibitions**

- Programs may not require households to participate in a religious service as a condition of receiving program assistance.
- Programs must not terminate or deny services to households based on refusal to participate in supportive services. Supportive services are helping or educational resources that include support groups, mental health services, alcohol and substance abuse services, life skills or independent living skills services, vocational services and social activities. Supportive services do not include housing stability planning or case management.
- Programs may not deny shelter to households that are unable to pay fees for shelter.
- If a program serves households with children, the age of a minor child cannot be used as a basis for denying any household’s admission to the program.
- If a program serves households with children, the program must serve all family compositions.
- If a program operates gender-segregated facilities, the program must allow the use of facilities consistent with the client’s gender expression or identity.
7.6 **Nondiscrimination**

As stated in the CHG Grant General Terms and Conditions Section 9 and Section 22, grantees must comply with all federal, state, and local nondiscrimination laws, regulations and policies.

Programs must comply with the Washington State Law against Discrimination, RCW 49.60, as it now reads or as it may be amended. RCW 49.60 currently prohibits discrimination or unfair practices because of race, creed, color, national origin, families with children, sex, marital status, sexual orientation, age, honorably discharged veteran or military status, or the presence of any sensory, mental, or physical disability or the use of a trained guide dog or service animal by a person with a disability.

Programs must comply with the Federal Fair Housing Act and its amendments as it now reads or as it may be amended. The Fair Housing Act currently prohibits discrimination because of race, color, national origin, religion, sex, disability or family status. The Fair Housing Act prohibits enforcing a neutral rule or policy that has a disproportionally adverse effect on a protected class.

Local nondiscrimination laws may include additional protected classes.

---

8 **Additional Requirements for Rapid Re-Housing and Targeted Prevention Programs**

8.1 **Washington Residential Landlord-Tenant Act**

Programs must provide information on the Washington Residential Landlord Tenant Act (RCW 59.18) to households receiving rent assistance.

For more information on this law, visit Washington Law Help, housing page, tenant rights at www.washingtonlawhelp.org

8.2 **Rent Limits**

Grantees must set a rent limit for their service area. The rent limit is the maximum rent that can be paid for a unit of a given size. Rent limit calculations must include the cost of utilities.

8.3 **Rental Agreements**

Client files must contain a rental agreement if rent assistance is paid on their behalf. If the rent assistance paid is move-in costs only, an Intent to Rent form is allowable.

8.4 **Targeted Prevention**

Programs that provide prevention assistance must use an evidence-based process to prioritize households most likely to become homeless.
9.1 Unsheltered Prioritization

Grantees must prioritize unsheltered homeless households for services and projects.

A household is considered in unsheltered priority status if they are:

- Currently living in a place not meant for habitation\(^8\)
- OR
- Currently fleeing violence: domestic violence, dating violence, sexual assault, stalking or other dangerous or life-threatening conditions that relate to violence against the individual or a family member
- OR
- Recently living in a place not meant for habitation or fleeing violence

Fulfilling this requirement can be demonstrated by:

- Achieving Functional Zero for at least two subpopulations
- OR
- Serving at least 60% Unsheltered Homeless households
- OR
- Increasing Percent of Unsheltered Homeless households 5 percentage points in each year of the contract period

9.1.1 Functional Zero

Grantees can meet the requirement to prioritize unsheltered homeless households by achieving Functional Zero for at least two subpopulations in the grantee’s service area.

Functional Zero is reached when the number of housing placements\(^9\) is equal to or greater than the number of current and newly identified homeless households\(^10\).

Subpopulations are:

- Youth\(^11\)
- Veterans
- Chronically Homeless
- Families with minor children
- Individual Adults (households without minor children)

---

\(^8\) Living outside or in a place that is not designed for, or ordinarily used as a regular sleeping accommodation for human beings, including a vehicle, park, abandoned building, bus or train station, airport, or campground.

\(^9\) The number of homeless households exited from Street Outreach, Emergency Shelter, Transitional Housing to permanent housing, AND the number of homeless households in any Permanent Housing type project (including Rapid Re-Housing) with a Housing Move-In during the report period.

\(^10\) The number of homeless households within a given community based on the best available data on each community’s homeless population. This can include the community’s “Active or By-Name List” or a combination of administrative data.

\(^11\) Unaccompanied youth under age 18
Commerce will evaluate grantees asserting Functional Zero based on state and local administrative data, and qualitative data gathered from key stakeholders. Evaluation will include confirmation that grantees meet the United States Interagency Council on Homelessness (USICH) criteria and benchmarks for each subpopulation.

Grantees may seek federal confirmation of Functional Zero, or ending homelessness among a subpopulation. If federally confirmed, Commerce will not provide evaluation.

Reaching Functional Zero is an accomplishment that requires maintenance. Confirmed Functional Zero is will not exempt the grantee from future requirements. Reconfirmation will be required for each contract cycle. If a grantee reaches and maintains Functional Zero two subpopulations, they will be required to focus on the remaining subpopulations.

### 9.1.2 Increase Percent of Unsheltered Homeless Households

Grantees can meet the requirement to prioritize unsheltered homeless households increasing percent served of unsheltered homeless households 5 percentage points in each year of the contract period.

Grantees that have not achieved functional zero for two subpopulations, and do not increase the percent served of unsheltered homeless households may assert that they have met a high performance threshold which will be evaluated by the Commerce based on state and local administrative data, and qualitative data gathered from key stakeholders.

### 9.1.3 Measurement

The Homeless Management Information System (HMIS) is the data source. Data for the previous state fiscal year will serve as the baseline. Compliance is measured at the system level. This means data from all applicable projects are included, without regard to fund sources.

1. **Client Universe:**
   Any head of household or adult who entered into Emergency Shelter, Safe Haven, Transitional Housing, Homelessness Prevention, or any permanent housing type project (including Rapid Re-Housing) during the report period.

2. **Count Unsheltered:**
   Of the client universe, count those with a prior residence (3.917A living situation): Place not meant for habitation OR answered 4.11 Domestic Violence YES AND YES to “Are you currently fleeing?”

3. **Count History of Unsheltered:**
   For the remaining client universe, count those who were active in any Emergency Shelter, Safe Haven, Transitional Housing, Homelessness Prevention, Street Outreach, Services Only, or any permanent housing type project (including Rapid Re-Housing) within 24 months prior to the reporting period AND had a prior residence (3.917A living situation) of: Place not meant for habitation OR answered 4.11 Domestic Violence “YES” AND “YES” to “Are you currently fleeing?”
4. **Calculation:**
Divide the total from steps two and three by the total from step 1 (client universe) to calculate the percent of people served who are considered in unsheltered priority status.

9.2 **Housing Outcome Performance Measures**
Grantees must maintain performance measures to help evaluate their effectiveness as they work to ensure that homelessness is rare, brief, and one time.

- HUD Homeless System Performance measures or a variation of these measures must be included in subgrantee agreements with applicable targets or benchmarks
- Subgrantee agreements or a performance management plan must describe the frequency of performance monitoring
- Subgrantee agreements or a performance management plan must describe actions taken if the performance expectations are not met

9.2.1 **Housing Outcome Performance Monitoring**
Commerce will monitor grantee SDG performance management activities. Grantees must provide the following upon request:

- Evidence of communicating performance outcomes with subgrantees through web-based dashboards, reports or other means
- Evidence of performance monitoring
- A description of performance monitoring outcomes including the number of projects with performance issues and specific actions taken (e.g. development of technical assistance plans, reduction in funding, etc.)
- A description of performance improvement strategies currently deployed or in development
To prevent lead-poisoning in young children, Lead/Subgrantees must comply with the Lead-Based Paint Poisoning Prevention Act of 1973 and its applicable regulations found at 24 CFR 35, Parts A, B, M, and R.

**Disclosure Requirements**

For ALL properties constructed prior to 1978, landlords must provide tenants with:

- Disclosure form for rental properties disclosing the presence of known and unknown lead-based paint;
- A copy of the “Protect Your Family from Lead in the Home” pamphlet.

Both the disclosure form and pamphlet are available at: [https://www.epa.gov/lead/realestate-disclosure](https://www.epa.gov/lead/realestate-disclosure)

It is recommended that rent assistance providers also share this information with their clients.

**Determining the Age of the Unit**

Lead/Subgrantees should use formal public records, such as tax assessment records, to establish the age of a unit. These records are typically maintained by the state or county and will include the year built or age of the property. To find online, search for your county name with one of the following phrases:

- “property tax records”
- “property tax database”
- “real property sales”

Print the screenshot for the case file. If not available online, the information is public and can be requested from the local authorities.

**Conducting a Visual Assessment**

Visual assessments are required when:

- The leased property was constructed before 1978; **AND**
- A child under the age of six or a pregnant woman will be living in the unit occupied by the household receiving CHG rent assistance.

A visual assessment must be conducted prior to providing CHG rent assistance to the unit and on an annual basis thereafter (as long as assistance is provided). Lead/Subgrantees may choose to have their program staff complete the visual assessments or they may procure services from a contractor. Visual assessments must be conducted by a HUD-Certified Visual Assessor. Anyone may become a HUD-Certified Visual Assessor by successfully completing a 20-minute online training on HUD’s website at: [http://www.hud.gov/offices/lead/training/visualassessment/h00101.htm](http://www.hud.gov/offices/lead/training/visualassessment/h00101.htm)
If a visual assessment reveals problems with paint surfaces, Lead/Subgrantees cannot approve the unit for CHG assistance until the deteriorating paint has been repaired. Lead/Subgrantees may wait until the repairs are completed or work with the household to locate a different (lead-safe) unit.

**Locating a Certified Lead Professional and Further Training**

To locate a certified lead professional in your area:

- Call your state government (health department, lead poison prevention program, or housing authority).
- Call the National Lead Information Center at 1-800-424-LEAD (5323).
- Go to the US Environmental Protection Agency website at https://www.epa.gov/lead and click on "Find a Lead-Safe Certified Firm."
- Go to Washington State Department of Commerce Lead-Based Paint Program website at http://www.commerce.wa.gov/building-infrastructure/housing/lead-based-paint/lead-based-paint-program-lbpabatement/ and click on “Find a Certified LBP Firm” under Other Resources.

Information on lead-based programs in Washington State can be found at http://www.commerce.wa.gov/building-infrastructure/housing/lead-based-paint/.

For more information on the Federal training and certification program for lead professionals, contact the National Lead Information Center (NLIC) at https://www.epa.gov/lead/forms/lead-hotline-national-lead-information-center or 1-800-424-LEAD to speak with an information specialist.

The Lead Safe Housing Rule as well as a HUD training module can be accessed at http://portal.hud.gov/hudportal/HUD?src=/program_offices/healthy_homes/enforcement/lshr
11 Appendix C: Access to the DSHS Benefits Verification System Data Security Requirements

1. Definitions. The words and phrases listed below, as used in this Appendix, shall each have the following definitions:
   a. “Authorized User(s)” means an individual or individuals with an authorized business requirement to access DSHS Confidential Information.
   b. “Hardened Password” means a string of at least eight characters containing at least one alphabetic character, at least one number and at least one special character such as an asterisk, ampersand or exclamation point.
   c. “Unique User ID” means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase or other mechanism, authenticates a user to an information system.
   d. “Contractor” means CHG Lead/subgrantees.

2. Data Transport. When transporting DSHS Confidential Information electronically, including via email, the Data will be protected by:
   a. Transporting the Data within the (State Governmental Network) SGN or Contractor’s internal network, or;
   b. Encrypting any Data that will be in transit outside the SGN or Contractor’s internal network. This includes transit over the public Internet.

3. Protection of Data. The Contractor agrees to store Data on one or more of the following media and protect the Data as described:
   a. Hard disk drives. Data stored on local workstation hard disks. Access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.
   b. Network server disks. Data stored on hard disks mounted on network servers and made available through shared folders. Access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism. For DSHS Confidential Information stored on these disks, deleting unneeded Data is sufficient as long as the disks remain in a Secured Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data as outlined in Section 5. Data Disposition may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.
   c. Optical discs (CDs or DVDs) in local workstation optical disc drives. Data provided by DSHS on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a Secured Area. When not in use for the contracted purpose, such
discs must be locked in a drawer, cabinet or other container to which only Authorized Users have the key, combination or mechanism required to access the contents of the container. Workstations which access DSHS Data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

d. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers.** Data provided by DSHS on optical discs which will be attached to network servers and which will not be transported out of a Secured Area. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

e. **Paper documents.** Any paper records must be protected by storing the records in a Secured Area which is only accessible to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

f. **Remote Access.** Access to and use of the Data over the State Governmental Network (SGN) or Secure Access Washington (SAW) will be controlled by DSHS staff who will issue authentication credentials (e.g. a Unique User ID and Hardened Password) to Authorized Users on Contractor staff. Contractor will notify DSHS staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Contractor, and whenever an Authorized User’s duties change such that the Authorized User no longer requires access to perform work for this Contract

g. **Data storage on portable devices or media.**

1. Except where otherwise specified herein, DSHS Data shall not be stored by the Contractor on portable devices or media unless specifically authorized within the terms and conditions of the Contract. If so authorized, the Data shall be given the following protections:
   
   (a) Encrypt the Data with a key length of at least 128 bits
   (b) Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics.
   (c) Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.

2. Physically Secure the portable device(s) and/or media by
   
   (d) Keeping them in locked storage when not in use
   (e) Using check-in/check-out procedures when they are shared, and
   (f) Taking frequent inventories

3. When being transported outside of a Secured Area, portable devices and media with DSHS Confidential Information must be under the physical control of Contractor staff with authorization to access the Data.

4. Portable devices include, but are not limited to; smart phones, tablets, flash
memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook/netbook computers if those computers may be transported outside of a Secured Area.

(4) Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape), or flash media (e.g. CompactFlash, SD, MMC).

h. Data stored for backup purposes.

(1) DSHS data may be stored on portable media as part of a Contractor’s existing, documented backup process for business continuity or disaster recovery purposes. Such storage is authorized until such time as that media would be reused during the course of normal backup operations. If backup media is retired while DSHS Confidential Information still exists upon it, such media will be destroyed at that time in accordance with the disposition requirements in Section 5. Data Disposition

(2) DSHS Data may be stored on non-portable media (e.g. Storage Area Network drives, virtual media, etc.) as part of a Contractor’s existing, documented backup process for business continuity or disaster recovery purposes. If so, such media will be protected as otherwise described in this exhibit. If this media is retired while DSHS Confidential Information still exists upon it, the data will be destroyed at that time in accordance with the disposition requirements in Section 5. Data Disposition.

4. Data Segregation.

a. DSHS Data must be segregated or otherwise distinguishable from non-DSHS data. This is to ensure that when no longer needed by the Contractor, all DSHS Data can be identified for return or destruction. It also aids in determining whether DSHS Data has or may have been compromised in the event of a security breach. As such, one or more of the following methods will be used for data segregation.

b. DSHS Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS data. And/or,
c. DSHS Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS Data. And/or,
d. DSHS Data will be stored in a database which will contain no non-DSHS data. And/or,
e. DSHS Data will be stored within a database and will be distinguishable from non-DSHS data by the value of a specific field or fields within database records.
f. When stored as physical paper documents, DSHS Data will be physically segregated from non-DSHS data in a drawer, folder, or other container.
g. When it is not feasible or practical to segregate DSHS Data from non-DSHS data, then both the DSHS Data and the non-DSHS data with which it is commingled must be protected as described in this exhibit.

5. Data Disposition. When the contracted work has been completed or when no longer needed, except as noted in Section 3. Protection of Data b. Network Server Disks above, Data shall be returned to DSHS or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:
6. **Notification of Compromise or Potential Compromise.** The compromise or potential compromise of DSHS shared Data must be reported to the Department of Commerce Contact designated in the Grant Agreement within one (1) business day of discovery.

**Data shared with Subcontractors.** If DSHS Data access provided under this Contract is to be shared with a subcontractor, the Contract with the subcontractor must include all of the data security provisions within this Contract and within any amendments, attachments, or exhibits within this Contract.

<table>
<thead>
<tr>
<th>Data Stored On:</th>
<th>Will be Destroyed By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portable hard disks) excluding optical discs</td>
<td>Using a “wipe” utility which will overwrite the Data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk</td>
</tr>
<tr>
<td>Paper documents with sensitive or Confidential Information</td>
<td>Recycling through a contracted firm provided the contract with the recycler assures that the confidentiality of Data will be protected.</td>
</tr>
<tr>
<td>Paper documents containing Confidential Information requiring special handling (e.g. protected health information)</td>
<td>On-site shredding, pulping, or incineration</td>
</tr>
<tr>
<td>Optical discs (e.g. CDs or DVDs)</td>
<td>Incineration, shredding, or completely defacing the readable surface with a coarse abrasive</td>
</tr>
<tr>
<td>Magnetic tape</td>
<td>Degaussing, incinerating or crosscut shredding</td>
</tr>
</tbody>
</table>
Appendix D: Access to the DSHS HEN Referral List Data Security Requirements

As required under RCW 43.185.C 230 and RCW 74.62.030, the Lead/sub grantee may use the HEN Referral List information for the sole purpose of improving access to HEN assistance for individuals determined eligible for a referral to HEN.

Access to Data shall be limited to staff whose duties specifically require access to such Data in the performance of their assigned duties.

Prior to making Data available to its staff, the Data Recipient shall notify all such staff of the Use and Disclosure requirements.

All staff accessing the data must sign a DSHS Nondisclosure of Confidential Information – Non Employee form prior to accessing the Data.

The Lead/sub grantee shall maintain a list of such staff and their signed DSHS Nondisclosure of Confidential Information – Non Employee forms. These forms must be updated annually and submitted to Commerce upon request.

Limitations on Use of Data: If the Data and analyses generated by the Lead/sub grantee contain personal information about DSHS clients, then any and all reports utilizing these Data shall be subject to review and approval by Commerce prior to publication in any medium or presentation in any forum.

1. Definitions. The words and phrases listed below, as used in this Exhibit, shall each have the following definitions:
   b. “Authorized Users(s)” means an individual or individuals with a business need to access DSHS Confidential Information, and who has or have been authorized to do so.
   c. “Business Associate Agreement” means an agreement between DSHS and a contractor who is receiving Data covered under the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996. The agreement establishes permitted and required uses and disclosures of protected health information (PHI) in accordance with HIPAA requirements and provides obligations for business associates to safeguard the information.
   d. “Category 4 Data” is data that is confidential and requires special handling due to statutes or regulations that require especially strict protection of the data and from which especially serious consequences may arise in the event of any compromise of such data. Data classified as Category 4 includes but is not limited to data protected

e. “Cloud” means data storage on servers hosted by an entity other than the Contractor and on a network outside the control of the Contractor. Physical storage of data in the cloud typically spans multiple servers and often multiple locations. Cloud storage can be divided between consumer grade storage for personal files and enterprise grade for companies and governmental entities. Examples of consumer grade storage would include iTunes, Dropbox, Box.com, and many other entities. Enterprise cloud vendors include Microsoft Azure, Amazon Web Services, and Rackspace.

f. “Encrypt” means to encode Confidential Information into a format that can only be read by those possessing a “key”; a password, digital certificate or other mechanism available only to authorized users. Encryption must use a key length of at least 256 bits for symmetric keys, or 2048 bits for asymmetric keys. When a symmetric key is used, the Advanced Encryption Standard (AES) must be used if available.

g. “FedRAMP” means the Federal Risk and Authorization Management Program (see www.fedramp.gov), which is an assessment and authorization process that federal government agencies have been directed to use to ensure security is in place when accessing Cloud computing products and services.

h. “Hardened Password” means a string of at least eight characters containing at least three of the following four character classes: Uppercase alphabetic, lowercase alphabetic, numeral, and special characters such as an asterisk, ampersand, or exclamation point.

i. “Mobile Device” means a computing device, typically smaller than a notebook, which runs a mobile operating system, such as iOS, Android, or Windows Phone. Mobile Devices include smart phones, most tablets, and other form factors.

j. “Multi-factor Authentication” means controlling access to computers and other IT resources by requiring two or more pieces of evidence that the user is who they claim to be. These pieces of evidence consist of something the user knows, such as a password or PIN; something the user has such as a key card, smart card, or physical token; and something the user is, a biometric identifier such as a fingerprint, facial scan, or retinal scan. “PIN” means a personal identification number, a series of numbers which act as a password for a device. Since PINs are typically only four to six characters, PINs are usually used in conjunction with another factor of authentication, such as a fingerprint.

k. “Portable Device” means any computing device with a small form factor, designed to be transported from place to place. Portable devices are primarily battery powered devices with base computing resources in the form of a processor, memory, storage,
and network access. Examples include, but are not limited to, mobile phones, tablets, and laptops. Mobile Device is a subset of Portable Device.

l. “Portable Media” means any machine readable media that may routinely be stored or moved independently of computing devices. Examples include magnetic tapes, optical discs (CDs or DVDs), flash memory (thumb drive) devices, external hard drives, and internal hard drives that have been removed from a computing device.

m. “Secure Area” means an area to which only authorized representatives of the entity possessing the Confidential Information have access, and access is controlled through use of a key, card key, combination lock, or comparable mechanism. Secure Areas may include buildings, rooms or locked storage containers (such as a filing cabinet or desk drawer) within a room, as long as access to the Confidential Information is not available to unauthorized personnel. In otherwise Secure Areas, such as an office with restricted access, the Data must be secured in such a way as to prevent access by non-authorized staff such as janitorial or facility security staff, when authorized Contractor staff are not present to ensure that non-authorized staff cannot access it.

n. “Trusted Network” means a network operated and maintained by the Contractor, which includes security controls sufficient to protect DSHS Data on that network. Controls would include a firewall between any other networks, access control lists on networking devices such as routers and switches, and other such mechanisms which protect the confidentiality, integrity, and availability of the Data.

o. “Unique User ID” means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase or other mechanism, authenticates a user to an information system.

2. **Authority.** The security requirements described in this document reflect the applicable requirements of Standard 141.10 ([https://ocio.wa.gov/policies](https://ocio.wa.gov/policies)) of the Office of the Chief Information Officer for the state of Washington, and of the DSHS Information Security Policy and Standards Manual. Reference material related to these requirements can be found here: [https://www.dshs.wa.gov/fsa/central-contract-services/keeping-dshs-client-information-private-and-secure](https://www.dshs.wa.gov/fsa/central-contract-services/keeping-dshs-client-information-private-and-secure), which is a site developed by the DSHS Information Security Office and hosted by DSHS Central Contracts and Legal Services.

3. **Administrative Controls.** The Lead/sub grantee must have the following controls in place:
   a. A documented security policy governing the secure use of its computer network and systems, and which defines sanctions that may be applied to Lead/sub grantee staff for violating that policy.

4. **Authorization, Authentication, and Access.** In order to ensure that access to the Data is limited to authorized staff, the Lead/sub grantee must:
   a. Have documented policies and procedures governing access to systems with the shared Data.
   b. Restrict access through administrative, physical, and technical controls to authorized staff.
c. Ensure that user accounts are unique and that any given user account logon ID and password combination is known only to the one employee to whom that account is assigned. For purposes of non-repudiation, it must always be possible to determine which employee performed a given action on a system housing the Data based solely on the logon ID used to perform the action.

d. Ensure that only authorized users are capable of accessing the Data.

e. **Ensure that an employee’s access to the Data is removed immediately:**
   1. Upon suspected compromise of the user credentials.
   2. When their employment is terminated.
   3. When they no longer need access to the Data.

f. Have a process to periodically review and verify that only authorized users have access to systems containing DSHS Confidential Information.

g. When accessing the Data from within the Lead/sub grantee’s network (the Data stays within the Lead/sub grantee’s network at all times), enforce password and logon requirements for users within the Lead/sub grantee network, including:
   1. A minimum length of 8 characters, and containing at least three of the following character classes: uppercase letters, lowercase letters, numerals, and special characters such as an asterisk, ampersand, or exclamation point.
   2. That a password does not contain a user’s name, logon ID, or any form of their full name.
   3. That a password does not consist of a single dictionary word. A password may be formed as a passphrase which consists of multiple dictionary words.
   4. That passwords are significantly different from the previous four passwords. Passwords that increment by simply adding a number are not considered significantly different.

h. When accessing Confidential Information from an external location (the Data will traverse the Internet or otherwise travel outside the Lead/sub grantee network), mitigate risk and enforce password and logon requirements for users by employing measures including:
   1. Ensuring mitigations applied to the system don’t allow end-user modification.
   2. Not allowing the use of dial-up connections.
   3. Using industry standard protocols and solutions for remote access. Examples would include RADIUS and Citrix.
   4. Encrypting all remote access traffic from the external workstation to Trusted Network or to a component within the Trusted Network. The traffic must be encrypted at all times while traversing any network, including the Internet, which is not a Trusted Network.
   5. Ensuring that the remote access system prompts for re-authentication or performs automated session termination after no more than 30 minutes of inactivity.
   6. Ensuring use of Multi-factor Authentication to connect from the external
end point to the internal end point.

i. Passwords or PIN codes may meet a lesser standard if used in conjunction with another authentication mechanism, such as a biometric (fingerprint, face recognition, iris scan) or token (software, hardware, smart card, etc.) in that case:

1. The PIN or password must be at least 5 letters or numbers when used in conjunction with at least one other authentication factor
2. Must not be comprised of all the same letter or number (11111, 22222, aaaaa, would not be acceptable)
3. Must not contain a “run” of three or more consecutive numbers (12398, 98743 would not be acceptable)

j. If the contract specifically allows for the storage of Confidential Information on a Mobile Device, passcodes used on the device must:

1. Be a minimum of six alphanumeric characters.
2. Contain at least three unique character classes (upper case, lower case, letter, number).
3. Not contain more than a three consecutive character run. Passcodes consisting of 12345, or abcd12 would not be acceptable.

k. Render the device unusable after a maximum of 10 failed logon attempts.

5. **Protection of Data.** The Lead/sub grantee agrees to store Data on one or more of the following media and protect the Data as described:

a. **Hard disk drives.** For Data stored on local workstation hard disks, access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

b. **Network server disks.** For Data stored on hard disks mounted on network servers and made available through shared folders, access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism. For DSHS Confidential Information stored on these disks, deleting unneeded Data is sufficient as long as the disks remain in a Secure Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data, as outlined below in Section 8 Data Disposition, may be deferred until the disks are retired, replaced, or otherwise taken out of the Secure Area.

c. **Optical discs (CDs or DVDs) in local workstation optical disc drives.** Data provided by DSHS on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a Secure Area. When not in use for the contracted purpose, such discs must be Stored in a Secure Area.
Workstations which access DSHS Data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

d. Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers. Data provided by DSHS on optical discs which will be attached to network servers and which will not be transported out of a Secure Area. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

e. Paper documents. Any paper records must be protected by storing the records in a Secure Area which is only accessible to authorized personnel. When not in use, such records must be stored in a Secure Area.

f. Remote Access. Access to and use of the Data over the State Governmental Network (SGN) or Secure Access Washington (SAW) will be controlled by DSHS staff who will issue authentication credentials (e.g. a Unique User ID and Hardened Password) to Authorized Users on Contractor’s staff. Contractor will notify DSHS staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Contractor, and whenever an Authorized User’s duties change such that the Authorized User no longer requires access to perform work for this Contract.

g. Data storage on portable devices or media.
(1) Except where otherwise specified herein, DSHS Data shall not be stored by the Lead/sub grantee on portable devices or media unless specifically authorized within the terms and conditions of the Grant. If so authorized, the Data shall be given the following protections:
(a) Encrypt the Data.
(b) Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics.
(c) Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.
(d) Apply administrative and physical security controls to Portable Devices and Portable Media by:
   i. Keeping them in a Secure Area when not in use,
   ii. Using check-in/check-out procedures when they are shared, and
   iii. Taking frequent inventories.

(2) When being transported outside of a Secure Area, Portable Devices and Portable Media with DSHS Confidential Information must be under the
physical control of Lead/sub grantee staff with authorization to access the Data, even if the Data is encrypted.

h. Data stored for backup purposes.
   (1) DSHS Confidential Information may be stored on Portable Media as part of a Lead/sub grantee’s existing, documented backup process for business continuity or disaster recovery purposes. Such storage is authorized until such time as that media would be reused during the course of normal backup operations. If backup media is retired while DSHS Confidential Information still exists upon it, such media will be destroyed at that time in accordance with the disposition requirements below in Section 8 Data Disposition.
   (2) Data may be stored on non-portable media (e.g. Storage Area Network drives, virtual media, etc.) as part of a Lead/sub grantee’s existing, documented backup process for business continuity or disaster recovery purposes. If so, such media will be protected as otherwise described in this exhibit. If this media is retired while DSHS Confidential Information still exists upon it, the data will be destroyed at that time in accordance with the disposition requirements below in Section 8 Data Disposition.

i. Cloud storage. DSHS Confidential Information requires protections equal to or greater than those specified elsewhere within this exhibit. Cloud storage of Data is problematic as neither DSHS nor the Lead/sub grantee has control of the environment in which the Data is stored. For this reason:
   (1) DSHS Data will not be stored in any consumer grade Cloud solution, unless all of the following conditions are met:
      (a) Lead/sub grantee has written procedures in place governing use of the Cloud storage and Contractor attests in writing that all such procedures will be uniformly followed.
      (b) The Data will be Encrypted while within the Lead/sub grantee network.
      (c) The Data will remain Encrypted during transmission to the Cloud.
      (d) The Data will remain Encrypted at all times while residing within the Cloud storage solution.
      (e) The Lead/sub grantee will possess a decryption key for the Data, and the decryption key will be possessed only by the Lead/sub grantee and/or DSHS.
      (f) The Data will not be downloaded to non-authorized systems, meaning systems that are not on either the DSHS or Lead/sub grantee networks.
      (g) The Data will not be decrypted until downloaded onto a computer within the control of an Authorized User and within either the DSHS or Lead/sub grantee’s network.
   (2) Data will not be stored on an Enterprise Cloud storage solution unless either:
      (a) The Cloud storage provider is treated as any other Sub-
Contractor, and agrees in writing to all of the requirements within this exhibit; or,  

(b) The Cloud storage solution used is FedRAMP certified.  

(3) If the Data includes protected health information covered by the Health Insurance Portability and Accountability Act (HIPAA), the Cloud provider must sign a Business Associate Agreement prior to Data being stored in their Cloud solution.

6. **System Protection.** To prevent compromise of systems which contain DSHS Data or through which that Data passes:
   a. Systems containing DSHS Data must have all security patches or hotfixes applied within 3 months of being made available.  
   b. The Lead/sub grantee will have a method of ensuring that the requisite patches and hotfixes have been applied within the required timeframes.  
   c. Systems containing DSHS Data shall have an Anti-Malware application, if available, installed.  
   d. Anti-Malware software shall be kept up to date. The product, its anti-virus engine, and any malware database the system uses, will be no more than one update behind current.

7. **Data Segregation.**  
   a. DSHS Data must be segregated or otherwise distinguishable from non-DSHS data. This is to ensure that when no longer needed by the Lead/sub grantee, all DSHS Data can be identified for return or destruction. It also aids in determining whether DSHS Data has or may have been compromised in the event of a security breach. As such, one or more of the following methods will be used for data segregation.  
      (1) DSHS Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS Data. And/or,  
      (2) DSHS Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS Data. And/or,  
      (3) DSHS Data will be stored in a database which will contain no non-DSHS data. And/or,  
      (4) DSHS Data will be stored within a database and will be distinguishable from non-DSHS data by the value of a specific field or fields within database records.  
      (5) When stored as physical paper documents, DSHS Data will be physically segregated from non-DSHS data in a drawer, folder, or other container.  
   b. When it is not feasible or practical to segregate DSHS Data from non-DSHS data, then both the DSHS Data and the non-DSHS data with which it is commingled must be protected as described in this exhibit.

8. **Data Disposition.** When the contracted work has been completed or when the Data is no longer needed, except as noted above in Section 5.b, Data shall be returned to DSHS or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:
<table>
<thead>
<tr>
<th>Data stored on:</th>
<th>Will be destroyed by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portable hard disks) excluding optical discs</td>
<td>Using a “wipe” utility which will overwrite the Data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk</td>
</tr>
<tr>
<td>Paper documents with sensitive or Confidential Information</td>
<td>Recycling through a contracted firm, provided the contract with the recycler assures that the confidentiality of Data will be protected.</td>
</tr>
<tr>
<td>Paper documents containing Confidential Information requiring special handling (e.g. protected health information)</td>
<td>On-site shredding, pulping, or incineration</td>
</tr>
<tr>
<td>Optical discs (e.g. CDs or DVDs)</td>
<td>Incineration, shredding, or completely defacing the readable surface with a coarse abrasive</td>
</tr>
<tr>
<td>Magnetic tape</td>
<td>Degaussing, incinerating or crosscut shredding</td>
</tr>
</tbody>
</table>

9. **Notification of Compromise or Potential Compromise.** The compromise or potential compromise of DSHS shared Data must be reported to COMMERCE and DSHS Privacy Officer at dshsprivacyofficer@dshs.wa.gov designated within one (1) business day of discovery. Lead/sub grantee must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.

10. **Data shared with Subcontractors.** If DSHS Data provided under this Grant is to be shared with a subcontractor, the Grant with the subcontractor must include all of the data security provisions within this Grant and within any amendments, attachments, or exhibits within this Grant. If the Lead grantee cannot protect the Data as articulated within this Grant, then the contract with the sub grantee must be submitted to COMMERCE for review and approval.
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, persons who are homeless, 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.

Grantees/sub grantees and the Department of Commerce agree as follows:

General Understandings:
In this Agreement, the following terms will have the following meanings:
"Client" refers to a consumer of services;
"Partner Agency" refers generally to any Agency participating in HMIS.
“Agency staff” refers to both paid employees and volunteers.
“HMIS” refers to the HMIS system administered by Commerce.
“Enter(ing)” or “entry” refers to the entry of any Client information into HMIS.
“Shar(e)(ing),” or “Information Shar(e)(ing)” refers to the sharing of information which has been entered in HMIS with another Partner Agency.
“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.
“Identified Information” refers to Client data that can be used to identify a specific Client. Also referred to as “Confidential” data or information.
“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.

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.

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 using the Interagency Data Sharing Agreement available through Commerce.

Confidentiality:
Agency will not:
enter information into HMIS which it is not authorized to enter; and
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.

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;

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.

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.

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 or for Clients fleeing domestic violence situations.

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.

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.

Information Collection, Release and Sharing Consent:
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.

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 may not sign the consent form for themselves.

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

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.

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

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 personally identified information will not be shared with other Partner Agencies or visible to the Agency staff within the system.

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.

**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.

**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.

**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.

**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:

**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.

**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/hmiswa) 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.

**Computers:** Security for data maintained in HMIS depends on a secure computing environment.

Agency agrees to allow access to HMIS only from computers which are:
- owned by Agency or approved by Agency for the purpose of accessing and working with HMIS;
- protected from viruses by commercially available virus protection software;
- protected with a software or hardware firewall;
- maintained to insure that the computer operating system running the computer 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 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. 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.

**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).

**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.

**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.

**Information Entry Standards:**
Information entered into HMIS by Agency will be truthful, accurate and complete to the best of Agency's knowledge.
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.
Agency will only enter information into HMIS database with respect to individuals that it serves or intends to serve, including through referral.
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.
Agency will not alter or over-write information entered by another Agency.

**Use of HMIS:**
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.
Agency may report non-identifying information to other entities for funding or planning purposes. Such non-identifying information shall not directly identify individual Clients.
Agency and Commerce will report only non-identifying information in response to requests for information from HMIS unless otherwise required by law.
Agency will use HMIS database for legitimate business purposes only.
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.
Agency will not use the HMIS database to defraud federal, state or local governments, individuals or entities, or conduct any illegal activity.

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

**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.

**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 if the parties only and this agreement creates no rights in any third party.

**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.

**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.

**Additional Terms and Conditions:**
Agency will abide by such guidelines as are promulgated by HUD and/or Commerce from time to time regarding administration of the HMIS. 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.

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

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. 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.