Snohomish County
Human Services

Homeless Management Information System (HMIS) Policies and Procedures –12th Revision

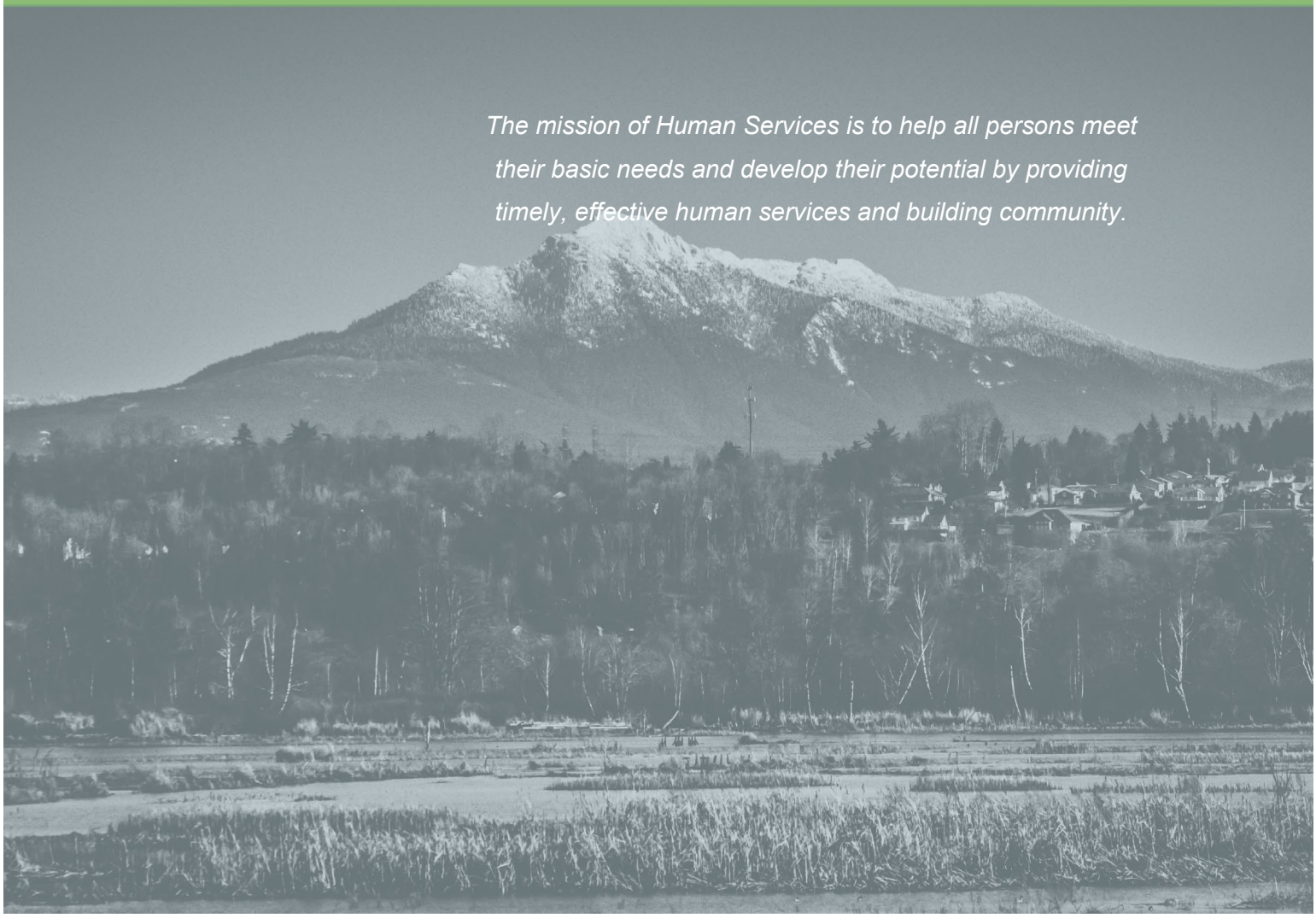

Table of Contents

Appendices

Exhibits

Document Revision History

Date	Edition	Comments
11/2015	Fifth	Appendix A: HMIS Data Elements and Definitions updated to reflect September 2015 version of 2014 HMIS Data Standards.
12/2016	Sixth	Appendix A: updated to reflect August 2016 version of 2014 HMIS Data Standards. Element 3.917 introduced References to Data Systems International changed to Eccovia Solutions as vendor name changed. Appendix C: HMIS Forms Overview updated to reflect changes in Consent and Release of Information forms. Allows for streamlined referral processes around Coordinated Assessment. Appendix H: Data Quality Plan updated with program and data entry averages. Document ends at Appendix H.
09/2017	Seventh	Section III (C): added Disaster Recovery information. Eccovia and Microsoft managed solution. (p.7 of 76). Section III (D): updated workstation requirements to include firewall and high-speed broadband. Language stating end users may not access HMIS via public Wi-Fi connection added. (p.8) Section IV: added language that Coordinated Entry and the Housing Roster is part of the HMIS platform, HMIS Administrator oversees these components. (p.8) Section V: Updated contacts list to include current County HMIS staff. Section VI: removed list of Partner Agencies, created link to County website for most current list. Updated County website to reflect current Partner Agencies (p.10) Section IX: Named Security Officer, expanded Reporting Security Incident and Security Violations subsections. Updated protocol for whom to contact if Security Officer is unreachable. (p.13) Appendix A: updated HMIS Data Elements and Definitions to reflect 2014 HMIS Data Standards, August 2016, version 5.1 release (pp.15-35) Appendix B (8a): updated to include language that Agencies must immediately notify HMIS Administrator is User employment is terminated. (p.41) Appendix D: updated Client Privacy Rights. (p.49) Appendix G: updated to document User start date and contact information. (p.56) Appendix H (2i): updated systems-wide benchmark table, including new elements and a great breakdown of those that are complete, unknown, refused, not collected, or missing (p.60) Appendix H (4) & (5a-e): frequency of monitoring and data correction directives updated (p.61) Appendix I: created in full, Monitoring of Data and HMIS Security. (pp.62-64) HMIS Annual Security Monitoring Checklist: created in full. (pp.65-66) Exhibit H: added existing sample Business Associate Agreement to HMIS Policies and Procedures manual. (pp.67-75)
01/2018	Eighth	Appendix A: updated HMIS Data Elements and Definitions to reflect 2017 HMIS Data Standards, July 2017, version 1.2 release effective October 1, 2017. (pp.15-32) Appendix H – Data Quality Plan: clarified “days” to mean “calendar days” for timeliness in data entry. (p.56) Exhibit H – HIPAA/Business Associate Agreement replaced with sample 2018 Business Associate Agreement. (pp.64-77)
06/2019	Ninth	Updated cover page and document formatting to department standards. Updated staff contact information throughout document. New ROI and Client Rights, effective January 2, 2019. (pp. 11-12, 44-50) Appendix H (4), Added information on Longitudinal Systems Analysis and Annual Commerce Golden. (p.57)

12/2021	Tenth	Updated language throughout for clarity and consistency. Updated contact information to direct to Snohomish County HMIS web page for current information. Appendix A: Removed element table and descriptions, and updated with a link to the current HMIS Data Standards Manual page, which is updated as new standards are published. (p. 14) Appendix H: Edited to align with updated procedure. (pp. 37-40) Appendix J: Added Snohomish County DQ Roles and Responsibilities Worksheet. (pp. 46-47)
2/2023	Eleventh	Clarified the expected timeline for annual monitoring from opening conference to closing.
3/2024	Twelfth	Updated pagination. Updated Section VII Participation Requirements – HMIS User Agreement: clarified review of user agreement and added requirements for HMIS users who have not accessed the database for defined periods of time. Clarified that user accounts must be created using a named/unique email address.

I. Introduction

The Snohomish County Homeless Management Information System (HMIS) is designed for agencies that provide housing and services to homeless individuals and families. The U.S. Department of Housing and Urban Development (HUD) under the Homelessness Housing and Assistance Act (RCW 43.185C) requires each Continuum of Care (CoC) to operate an HMIS and meet all requirements. Programs targeted for participation include coordinated entry, outreach services, supportive services for homeless persons, homelessness prevention and intervention, emergency shelter, transitional housing, rapid rehousing, permanent supportive housing, and other permanent housing. Beyond meeting the HUD requirements, it is our goal that HMIS assist agencies in recording and tracking client data and generating reports, providing helpful information to funders, planners, and policy makers, and to increase coordination among agencies.

A. Mission Statement

The mission of Snohomish County HMIS is to identify gaps in homeless services delivery, provide reporting resources for homeless services providers and funders, reduce duplicate efforts for both providers and recipients of homeless services, and facilitate access to services for persons who are homeless or at imminent risk of becoming homeless.

B. Benefits of the HMIS

- Inform government and the community about the extent and nature of homelessness in Snohomish County.
- Assist in numerous planning processes including but not limited to the 10-year plan to End Homelessness, CoC planning, and the Consolidated Plan.
- Enable agencies to have accurate information about the clients they serve.
- Provide information on successes and challenges of homeless programs.
- Prepare informational reports for funders.
- Facilitate funding needed for housing and other related services, thereby ultimately benefiting homeless households.
- Enable participating agencies and the community to understand client needs, resources, and gaps through the use of aggregated data.
- Help programs identify processes that are problematic, support redesign efforts, and improve the quality of the services provided by the organization.

C. Benefits of Using the HMIS

- Automated reporting – complete monthly, quarterly, and annual reports for key funders (including local funders, Washington State and HUD).
- No technical expertise or IT staff required – the HMIS is centrally-maintained and training is provided for all staff by Snohomish County HMIS Administrators.
- Designed to meet HUD, Health Insurance Portability and Accountability Act (HIPAA), and local provider needs.
- Captures changes in client needs over time.
- Enables client data sharing between HMIS Partner Agencies when programs and clients agree, eliminating redundant intake forms for clients and service providers.

D. Overview of the Snohomish County HMIS

HMIS Lead	Snohomish County Human Services Department is the entity designated by the Partnership to End Homelessness to operate the Continuum of Care's HMIS on its behalf.
HMIS Administrator	Snohomish County Human Services Department manages the HMIS implementation in Snohomish County by enrolling programs and managing appropriate use, supporting users through connection to, or direct provision of, User training, and overseeing system setup.
HMIS Software	ClientTrack is the HMIS Software used by the Snohomish County HMIS.
HMIS Software Vendor	Eccovia Solutions is the HMIS Software Vendor for ClientTrack.
HMIS Partner Agencies	Partner Agencies, also referred to as Covered Homeless Organizations (CHOs), Agencies or Participating Agencies, are the organizations that record, use, or process data on homeless clients for the HMIS.
HMIS Users	HMIS Users are the Agency staff persons who record, use, or process data on homeless clients for the HMIS.

II. Stages of Implementation

STAGE 1: Initiating Agency HMIS Participation (for new Agencies)

1. Agency completes and submits to Snohomish County Human Services Department all participation agreement materials including:
    - HMIS Agency Partner Agreement
      (see Appendix B – HMIS Agency Partner Agreement).
    - Signed HMIS User Agreement form for each individual agency end-user
2. An Internet connection—high speed broadband with hardwired connection and a static IP address–is secured for the agency. Agency is required to set up and maintain a firewall on this connection.
3. An Agency Site HMIS Contact is designated by Snohomish County HMIS Administrators.
4. The Agency Site HMIS Contact designates agency staff to receive access to the system.
5. Complete the training on use of forms (HMIS Informed Consent and Release of Information Authorization (ROI), Client Privacy Rights – see Appendix C – HMIS Forms Overview).
6. Complete all HMIS system training.
7. HMIS Administrators travel to the agency for a follow-up to assist the Agency Site HMIS Contact in initial operative tests on the program's equipment and completeness of security checklist (as needed).

STAGE 2: Data Entry Begins

1. The Agency Site HMIS Contact and site users receive training on uses of the HMIS application, including testing in temporary environment as necessary.
2. Usernames and temporary passwords are assigned for all end-users. Users are required to reset their password upon the initial entry into the system.
3. Data entry begins and includes the required data elements per the current HUD HMIS Data Standards.

4. HMIS Administrators are available for a site visit to assist with any questions after initial use of system.
5. HMIS Administrators track problems, opportunities to improve the process, and track coverage.

STAGE 3: System Fully Integrated in Daily Operation

1. Agency-specific training is provided on querying reports and additional functions accessed in Client Track.
2. Participating Agency begins using the information for internal evaluation and reporting requirements.

III. Maintenance of Data and Onsite Computer Equipment

A. Policy

Participating Agencies must commit to a reasonable program of data and equipment maintenance in order to sustain an efficient level of system operation.

B. Standard

Participating Agencies must meet the technical standards for minimum computer equipment configuration, internet connectivity, data storage, and data backup.

C. Responsibilities

The Partner Agency staff or designee will be responsible for the maintenance and disposal of on-site computer equipment and data used for participation in the HMIS as follows:

- **Computer Equipment:** Each Agency is responsible for maintenance of their computer equipment. This includes purchase of and upgrades to all existing and new computer equipment for utilization in HMIS.
- **Backup:** Eccovia Solutions is responsible for supporting a backup procedure for the server(s) on which the HMIS database resides.
- **Internet Connection:** Participating Agencies are responsible for troubleshooting problems with their agency's internet connections.
- **Data Storage:** Eccovia Solutions is responsible for storing data in a secure format and for performing daily backups of the data.
- **Data Disposal:** Participating Agencies are responsible for disposing of documents that contain identifiable client level data by shredding paper records, deleting any information from any recording media used to retain digital data before disposal, and deleting any copies of client level data from the hard drive of any machine before transfer or disposal.
    - **Retention of paper copies of personally identifying information:** Participating Agencies and the County may not retain paper copies of personally identifying information derived from HMIS longer than seven (7) years after the last day the person is served by the Agency. Paper copies will be destroyed through the use of a paper shredder or through a contract with a shredding management company.
- **Disaster Recovery:** Eccovia Solutions in coordination with Microsoft is responsible for coordinating disaster recovery. This is accomplished by hosting the ClientTrack platform within the Microsoft Azure cloud. In the event of a datacenter failure or loss, replication of virtual servers, the database platform and stored data can be migrated to a secondary Microsoft managed datacenter.
    - **In the event of an extended outage**: HMIS Lead will contact Agencies and Users to inform them of the event, what is being done to resolve the issue and expected time to resolution.

D. Minimum Workstation Requirements

User's computers must have, at a minimum, a high-speed broadband with hardwired connection to the internet. Agency is required to set up and maintain a firewall on this connection. Users may opt to use secure Wi-Fi connection owned, managed, and monitored by their agency's information technology department. Users may not, at any time, use a public Wi-Fi connection to access the HMIS platform. Operation of ClientTrack is dependent on the browser, not on the operating system installed on the computer. Per the vendor, ClientTrack is compatible with newer versions of the Google Chrome, Firefox, and Microsoft Edge web browsers.

E. Confidentiality

Confidentiality of the data in the system is of the utmost importance. The information in this system is confidential. Confidential information is sensitive or secret information, or information whose unauthorized disclosure could be harmful or prejudicial. Only those who have been explicitly granted their own username and password by the HMIS Administrators may access this system. Any printed information obtained from this system must also be treated as confidential.

IV. Roles and Responsibilities

Snohomish County HMIS Administrators are responsible for:

- System Administration of the platform to include HMIS projects, including Coordinated Entry.
- Authorizing usage and access to the HMIS.
- Limiting access to Users who need access to the system for technical administration, data entry, editing of client records, viewing of client records, report writing, administration of other essential activity associated with carrying out HMIS responsibilities.
- Developing reports and presenting data.
- Mining the database to respond to the information needs of participating organizations, community stakeholders and consumers.
- Documenting work on the database and in development of reports/queries.
- Provision of technical assistance as needed with program sites.
- Providing training to participating organizations on policies and procedures, system use, authorizing access to the system including set-up, in response to questions from users, and in response to network and system functionality questions.
- Coordinating technical support for the system.
- Communicating with participants regarding problems with entry and to support data quality.
- Monitoring agency participation including timeliness and completeness of entry.
- Communicating any planned or unplanned interruption in service.
- Reviewing and communicating as needed pertaining to the agencies' bi-monthly quality assurance reports.
- Auditing Policy and Procedure compliance.

Eccovia Solutions is responsible for:

- Administration of the internal network.
- Administration of product servers including web and database.
- Monitoring access to these systems through auditing.
- Monitoring functionality, speed, and database backup procedures.

- Backup and recovery of internal and external networks.
- Operating the system website twenty-four hours a day, seven days a week.
- Communicating any planned or unplanned interruption of service to an HMIS Administrator.

Agencies are responsible for:

- Notifying HMIS Administrators of any new projects dedicated to serving homeless clients.
- Notifying HMIS Administrators of any new public funding received, regardless of source.
- Providing to HMIS Administrators new project setup start dates, funding sources, project type, services to be tracked, unit types and any other special considerations.
- Notifying HMIS Administrators of any changes to existing projects to include funding sources, project type, services, unit types and any other special considerations.
- Notifying HMIS Administrators when the agency has a change in users, including new users and those whose HMIS access rights need to be revoked for any reason, including change in job duties or termination of employment.

All Snohomish County Users and County Staff users are responsible:

- To be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure.
- For reporting security violations.
- For complying with relevant policies and procedures.
- For their actions and for any actions undertaken with their usernames and passwords.

V. Snohomish County Contacts

To find current Snohomish County HMIS Admin contact information, please refer to the Snohomish County HMIS web page.

VI. Snohomish County HMIS Partner Agencies

The following list of Partner Agencies is subject to change; refer to the Snohomish County HMIS web page for the most current list.

VII. Participation Requirements

Agencies may not use the HMIS system, participation, or data as a reason to deny services or housing to a client.

A. Policy

Participating agencies must agree to use the following procedures in implementing their HMIS system at an agency level.

B. Training

Adhere to the commitment of Agency User(s) and designated staff person(s) to attend training(s) prior to accessing the system online. In the event the Agency User(s) change, then the new User(s) must attend training before accessing the HMIS system. Training can be coordinated by contacting an HMIS Administrator.

The basic training provided to Participating Agencies will, at minimum, include the following:

- Introduction to the HMIS;
- Review of applicable policies and procedures, including relevant security policies;
- Connecting to the internet;
- Logging on to the HMIS;
- Entering client information including data from Enrollment, Assessments, and Exit;
- Ensuring good quality data;
- Overview of system administrative functions;
- Entering and updating information pertaining to the Participating Agency;
- Oversight of data quality;
- Sessions will be designed and coordinated by Snohomish County HMIS Administrators; and
- Advanced training will be provided as requested by individual agencies.

C. HMIS User Agreement

- Each User must sign a Snohomish County HMIS User Policy, Code of Ethics and Responsibility Statement (Appendix C – HMIS Forms Overview) user agreement stating full understanding of system rules and protocols before receiving a username and password to access the system. These agreements will be reviewed at least annually.
- Each User must receive training in the use of the HMIS system from an HMIS Administrator.
- Agencies will request the number of Users accessing the HMIS system; each User must have their own individual username and password and must not share that information with anyone else. Sharing is strictly prohibited; accounts will not be created for positions/roles, but must be created using a named and unique agency email address.
- Agency Directors must approve each individual User from their agency.
- Access permission is contingent on continued employment at the agency, and will be terminated immediately if the User is no longer employed by the agency.
- Agency will notify an HMIS Administrator immediately if a User terminates employment so access rights may be revoked.
- User accounts that have been inactive for more than 30 days will be automatically deactivated. Users can only regain access by submitting an HMIS User Account Request form (found on the HMIS Training Resources webpage here: https://snohomishcountywa.gov/6320/HMIS-Training-Resources).
- Users who have not accessed the database for six months or more will be required to complete the HMIS Security Training before regaining access.

D. Data Protocols

- Only authorized Users may view or update client data.
- Each head of household and adult member of a household that is receiving housing or services will be expected to review and be given the opportunity to sign the HMIS Informed Consent and ROI.
- Consent for data entry for accompanied minors will be provided by the parent/guardian.

- If a client refuses entry of identified information into HMIS, the Agency must have a mechanism in place to track the entry of de-identified information.
    - Additionally, the Agency will only use the first name, last name combination of "Anonymous, Anonymous," and nothing else (ex: "John Doe" is not allowed) for de-identified clients. The Agency will follow guidance to de-identify other Personally Identifiable Information (PII) per the current Snohomish County HMIS Data Entry Manual.
- Clients always retain the right to view their own data and request corrections.

E. Aggregate Data Sharing and Release

- Each Agency, in partnership with Snohomish County, owns the client data for housing and/or services provided by them.
- Agencies are encouraged to use their own HMIS data for public relations, reporting and funding as long as client confidentiality is maintained.
- Aggregate HMIS homeless data (not client specific) will be published at an interval (TBD) by Snohomish County HMIS. Any Agency may use published HMIS data.
- Snohomish County staff may use HMIS data for planning, research and analysis, reporting, and grant writing processes including the Continuum of Care application, the Consolidated Plan, HUD reporting, etc., and may reconcile and release aggregate data.
- Client confidentiality must be upheld, and a signed release must specify that the client agrees to have their data shared with other HMIS Partner Agencies.

F. Participation Agreement and Standards

Agencies are required to sign a participation agreement stating their commitment to adhere to the policies and procedures for effective use of the system and proper collaboration with HMIS.

- Universal and Program Data Elements are to be entered into HMIS system within five (5) calendar days of a residential enrollment.
- Additional services and program-specific data is to be entered into the HMIS system within five (5) calendar days of the client exiting the housing stay or receiving a services only service.
- Quality assurance reports must be generated bi-monthly to verify data quality.
- Client identified information entered in HMIS must be based on the HMIS Consent and Release of Information and cannot be based on Agency policy.

VIII. Privacy Plan

A. HMIS Consent and Release of Information (ROI) Forms

These must be signed by clients to authorize the entry and sharing of their personal information electronically with other Participating Agencies through the HMIS where applicable.

B. Posting of the HMIS Client Privacy Rights Workstation Requirements

The HMIS Client Privacy Rights must be posted and clearly visible to clients at any data collection station.

C. Individual Data Sharing, Release, and Confidentiality

By signing the most recent HMIS Informed Consent and Release of Information Authorization, clients consent to their personal information being entered and shared with HMIS Partner Agencies. There are no longer differing options for sharing information; if data is entered, it is also able to be shared. If a client refuses consent, then they will be entered anonymously. Anonymous records will be shared as well.

D. Grievance Procedure

A client has the right to appeal his or her individual issues related to HMIS in accordance with Agency-dictated grievance policy. If no grievance procedure is in place as it relates to HMIS, it may be appealed by the following progression:

1. Agency Case Worker
2. Agency Case Worker's Supervisor
3. Agency Executive Director

IX. Security Plan

A. Policy

Access to all of computing, data communications, and sensitive data resources will be controlled. Access is controlled through User identification and authentication. Users are responsible and accountable for work done under their personal identifier (username). Access control violations must be monitored, reported to the Security Officer, and resolved. Agency staff will work to ensure that all sites receive the security benefits of the system while complying with all written policies.

B. Physical Security

Agencies must develop rules to address unattended workstations and physical access to workstations which minimize the risk of confidential data being accessed by unauthorized persons. Monitors displaying client data must be oriented to minimize viewing by unauthorized people.

C. Access to data

1. **User Access:** Users will be able to view only the data entered by Users of their own Agency or shared client records. Security measures exist within the HMIS system that restrict Agencies from viewing each other's data without permission.
2. **Raw Data:** Users can perform reporting functions which will address each Agency and programs' individual data.
3. **Agency Policies Restricting Access to data:** Each Partner Agency must establish internal access to data protocols. These policies should include who has access and for what purpose, prohibition of User account sharing, and how users can securely and appropriately transmit deidentified information. Other issues to be addressed include storage, transmission, and disposal of these data.

D. Reporting Security Incidents

The HMIS Administrator designates the Data and Program Analyst Lead as the Security Officer. Should a User have concern that a security incident occurred and/or client privacy has been compromised, the User must immediately report their concern to the Security Officer who will investigate. The current Data and Program Analyst Lead is identified on the Snohomish County HMIS web page.

In the event the Security Officer is unreachable, Users are to contact any Snohomish County HMIS staff member who will follow up with designated supervisor.

These Security Standards and associated Policies and Procedures are intended to prevent, to the greatest degree possible, any security incidents.

E. Security Violations

If during the course of investigation the Security Officer finds the suspected security or privacy concern resulted from a User's suspected or demonstrated noncompliance with the HMIS Partner Agency Agreement or HMIS User Policy, Code of Ethics, Responsibility Statement or best practices, the User's HMIS access will be revoked at least temporarily until the investigation is completed.

Following the investigation, the Security Officer will notify Leadership of any substantiated incidents that may have compromised the HMIS system and/or client privacy whether or not a release of client data is definitively known to have occurred. If the security or privacy concern resulted from demonstrated noncompliance by a User, regardless of intent, the Security Officer reserves the right to permanently revoke User HMIS access.

Within one business day after the Security Officer receives notice of the security or privacy concern, the Security Officer and Leadership will jointly establish an action plan to analyze the source of the security or privacy concern and actively prevent such future concerns. The action plan shall be implemented as soon as possible after the incident.

If the Partner Agency is not able to demonstrate the ability to prevent future occurrences of the incident or follow the action plan, the Security Officer in consultation with Leadership may elect to terminate the Partner Agency's access to HMIS. The Partner Agency may appeal to Leadership for reinstatement to HMIS following completion of the requirements set forth in the action plan.

In the event of a substantiated release of a client's Personal Identifiable Information in noncompliance with the provisions of these security standards, the Security Officer shall make a reasonable attempt to notify all impacted persons at the Agency's expense. The Security Officer shall notify other agencies, Leadership, Washington State Department of Commerce, and any other interested partners of the security incident. This notification process is designed to lessen impact, educate Users, prevent future occurrences, and instill confidence in security of the HMIS platform.

The HMIS Administrator shall maintain a record of all substantial releases of Personal Identifiable Information in noncompliance with the provisions of these security standards for seven (7) years.

Appendix A

HMIS Data Elements and Definitions

Partner Agencies are required to enter all Universal and applicable Program-Specific data elements included in the most recent version of the HUD HMIS Data Standards. In general, these Data Standards are updated every other year, and the current version can be found on HUD's HMIS Data Standards web page. Additional elements may be required for local funding reporting purposes. Technical guidance on entering these elements into the HMIS can be found in the most recent version of Snohomish County's Data Entry Manuals.

Appendix B

HMIS Agency Partner Agreement

This agreement (the "Agreement") is entered into between Snohomish County, a political subdivision of the State of Washington (the "County"), and _____, a Washington non-profit corporation (the "Agency"), for the purpose of implementing and/or maintaining the Snohomish County Homeless Management Information System ("HMIS") and is effective as provided in Section 16 hereof.

RECITALS

WHEREAS, in "Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice" (Docket No. FR 4848-N-02), 69 Fed. Reg. 45,887 (July 30, 2004) (the "HUD Final Notice"), the United States Department of Housing and Urban Development ("HUD") implemented national data and technical standards for locally administered homeless management information systems; and

WHEREAS, the HUD Final Notice required all recipients of McKinney-Vento Act (42 U.S.C. § 11301 et seq.) program funds and Housing Opportunities for People with AIDS (42 U.S.C. § 12901 et seq.) ("HOPWA") homeless funds from HUD to provide information on their progress in developing and implementing their homeless management information systems ("HMIS") and announced that that information would be used to determine annual program funding; and

WHEREAS, the County is a recipient of HUD McKinney-Vento Act program funds; and

WHEREAS, by Chapter 484, § 6, Laws of 2005, the State of Washington Department of Commerce, Trade and Economic Development ("CTED") was directed by the Washington legislature to conduct an annual Washington homeless census or count and, by the end of four years, to implement an online information and referral system to enable local governments and providers to identify available housing for homeless persons; and

WHEREAS, by Chapter 349, § 8, Laws of 2006, CTED was directed by the Washington legislature to implement a state-wide homeless client management information system by December 31, 2009, and to update that system with new homeless client information at least annually; and

WHEREAS, by Chapter 565, § 17, Laws of 2009, the Washington legislature changed the name of CTED to the Department of Commerce ("Commerce"); and

WHEREAS, Commerce requires data from all Washington counties in order to comply with state HMIS requirements under RCW 43.185C.180 and RCW 43.185C.030; and

WHEREAS, pursuant to an Interagency Data Sharing Agreement, dated August 9th, 2010, the County will provide the required HMIS data to Commerce at least quarterly via secure electronic file data transfer (data integration) using the federal data integration XML export standard; and

WHEREAS, the County has implemented software known as Client Track for the purpose of providing, hosting and maintaining its HMIS; and

WHEREAS, the purpose of this Agreement is to collect and maintain information regarding the characteristics and service needs of homeless clients for a variety of reasons, including the provision of more effective and streamlined services to clients and the creation of information which communities can use to determine the use and effectiveness of services; and

WHEREAS, 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; and

WHEREAS, the County has requested the Agency, and the Agency has agreed, to enter into this Agreement to reflect both the County's implementation of the Client Track software for its HMIS system and meet the new requirements imposed upon Commerce by RCW 43.185C.180 and RCW 43.185C.030;

NOW, THEREFORE, in consideration of the mutual covenants and promises herein contained, the Agency and the County agree as follows:

1. Definitions.

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

(i) "Agency staff" refers to paid employees.

(ii) "Client" refers to a consumer of services or, as appropriate to the context, the parent or legal guardian of that consumer of services.

(iii) "Client Track" refers to the software adopted by the County for the purpose of providing, hosting and maintaining its HMIS.

(iv) "Data sharing" or "information sharing" or "sharing" refers to the sharing with another Partner Agency or other Partner Agencies of information which has been entered into HMIS.

(v) "De-identified information" (also referred to as "non-identifying" information) refers to data that has specific client demographic information removed, allowing use of the data without identifying a specific client.

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

(vii) "Identified information" refers to data that has specific client information available for viewing, allowing the use of data that identifies a specific client.

(viii) "HMIS" refers to the homeless management information system maintained by Snohomish County or, when appropriate to the context, the Washington State HMIS into which Snohomish County HMIS information will be transferred.

(x) "Partner Agency" or "Partner Agencies" refers generally to an agency or those agencies participating in the Snohomish County HMIS.

(xi) "State" means the State of Washington acting by and through its Department of Commerce.

(xii) "User" refers to Agency employees or Agency volunteers authorized by the Agency to have, and having, access to HMIS.

2. Confidentiality.

A. The Agency understands that when it enters information into HMIS, such information will be available to County staff who may review the data to administer HMIS and will be available to County and State staff to conduct analysis and to prepare reports which may be submitted to others in de-identified form *without* individual identifying client information.

B. The Agency understands that it will have the responsibility to indicate whether information the Agency is entering into HMIS will be shared with and made accessible to Partner Agencies in HMIS. The Agency's indication of whether entered data will be shared must be based on selections made by the Client in the HMIS Informed Consent and Release of Information Authorization Form attached hereto as Exhibit B and incorporated herein by this reference.

C. The Agency will not:

(i) Enter information into HMIS which it is not authorized by a Client to enter; or

(ii) Designate information for sharing which the Agency is not authorized by a Client to share,

In each case 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, the Agency represents that it has the authority to enter such information into HMIS or to designate it for sharing, as the case may be.

D. The Agency represents that: *(check applicable items)*

(i) It is ___ **or** is not _____a "covered entity" whose disclosures are restricted under the Health Insurance Portability and Accountability Act of 1996, as amended, codified at 42 U.S.C. §§ 1320d-d8, and its implementing regulations at 45 CFR Parts 160 and 164 ("HIPAA").

(ii) It is ___ **or** is not ____ a program whose disclosures are restricted under the Federal Drug and Alcohol Confidentiality Regulations, 42 CFR Part 2 ("Confidentiality Regulations").

(iii) If the Agency is subject to HIPAA or the Confidentiality Regulations, a fully executed Business Associate or Business Associate/Qualified Service Organization Agreement must be attached to this Agreement before information may be entered into HMIS. Sharing of information will not be permitted otherwise.

(iv) If the Agency is subject to any laws or requirements which restrict Agency's ability either to enter or to authorize sharing of information, the Agency will ensure that any entry it makes in HMIS and all designations for sharing fully comply with all applicable laws or other restrictions (including but not limited to Section 605 of the Violence Against Women and Department of Justice Reauthorization Act of 2005 (Pub. L. 109-162), codified at 42 U.S.C. § 11383(a)(8); the HUD Final Notice; the "Homeless Management Information Systems (HMIS) Data and Technical Standards Final Notice; Clarification and Additional Guidance on Special Provisions for Domestic Violence Provider Shelters" (Docket No. FR 4848-N-03) promulgated by HUD, 69 Fed. Reg. 61,517 (October 19, 2004); and RCW 43.185C.030).

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

3. Display of Notice. Pursuant to the HUD Final Notice, the Agency will prominently display at each intake desk (or comparable location) a copy of the ***HMIS Client Privacy Rights*** that explains generally the reasons for collecting identified information in the HMIS and the client rights associated with providing Agency staff with identified data. Agency will post the ***HMIS Client Privacy Rights*** document prominently to ensure clients' understanding of their rights. The current form of ***HMIS Client Privacy Rights***, attached as Appendix A to and incorporated into this Agreement by this reference, may be modified from time to time by the County.

4. Information Collection, Release and Sharing Consent; Denial or Revocation of Consent.

A. *Collection of identified information.* An agency may collect 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 or required by law, with the knowledge or consent of the Client.

B. *Obtaining Client consent.* In addition to posting the ***HMIS Client Privacy Rights*** document prominently at each intake desk (or comparable location) as required by Section 3 of this Agreement, the Agency will obtain from each Client whose identified information is to be entered into HMIS a signed written consent in the form of the ***HMIS Informed Consent and Release of Information Authorization Form*** attached hereto as Appendix E. The signed ***HMIS Informed Consent and Release of Information Authorization Form*** must be obtained from the individual Client before data entry for that Client can begin. The ***HMIS Informed Consent and Release of Information Authorization Form*** may be modified from time to time by the County.

C. *Duration of Client consent.* As provided in RCW 43.185C.180(2), the consent of the Client must be reasonably time limited. The Agency shall confirm that the Client's consent has not been revoked or expired or lapsed prior to entering subsequent data for that Client into HMIS.

D. *Client denial of consent to entry of identified information.* If a Client denies consent for entry of some or all of his or her identified information in HMIS, the Agency will have the Client make the appropriate selections in the ***HMIS Informed Consent and Release of Information Authorization Form*** and sign it. The identified information of a Client who refuses to or otherwise does not sign the ***HMIS Informed Consent and Release of Information Authorization Form*** shall not be entered into HMIS.

E. *Client denial of data sharing.* If a Client denies consent for sharing of his or her identified information in HMIS with other Partner Agencies, the Agency will have the client make the appropriate selections in the ***HMIS Informed Consent and Release of Authorization Form*** and sign it.

F. *Withdrawal, revocation or expiration of consent.*

(i) A Client may withdraw or revoke his or her consent for identified information collection by signing the ***Client Revocation of HMIS Consent*** form attached hereto as Appendix F and incorporated herein by this reference. If a Client revokes his or her consent, the Agency is responsible for immediately making appropriate data entries in HMIS to ensure that Client's identified information is removed from HMIS.

(ii) When a Client's consent has by its terms expired, the Agency is responsible for securing a new written consent from the Client in the form of Appendix E. Absent the securing of a new written Client consent, the Client record associated with the Agency will be removed from HMIS automatically by the program known as Client Track at the conclusion of the seven (7) year retention period.

G. *Agency responsibilities.*

(i) In order to ensure that the consent obtained from clients will be knowing and informed, the Agency shall provide assistance before signature to each client who requires it with reading and understanding the ***HMIS Informed Consent and Release of Information Authorization Form***. Furthermore the Agency will arrange for a qualified interpreter/translator if the individual is not literate in English or has difficulty understanding the ***HMIS Client Privacy Rights*** or the associated consent forms.

(ii) It is the responsibility of the Agency entering information about a client to determine whether consent has been obtained; to make appropriate entries in HMIS either to designate the information as appropriate for sharing or to prohibit sharing; to implement any restrictions on information sharing, including those related to the duration of Client consents to information sharing; and to implement any withdrawal or revocation of consent to information sharing.

(iii) The Agency shall keep the originals of each client-signed ***HMIS Informed Consent and Release of Information Authorization Form*** for a period of seven (7) years after signature. The Agency shall make those signed forms available for inspection and copying by the County at any time.

5. No Conditioning of Services. The Agency will not condition any services upon or decline to provide any services to a Client based upon that Client's (a) refusal or failure to sign an ***HMIS Informed Consent and Release of Information Authorization Form,*** (b) refusal to agree to the entry into HMIS of his or her identified information, or (c) refusal to consent to the sharing of his or her identified information with Partner Agencies.

6. Re-release Prohibited. The Agency agrees not to release any identified information received from HMIS to any other person or organization unless consented to in writing by the client or required by law.

7. Client Inspection/Correction. The Agency will allow a Client to inspect and obtain a copy of his or her own personal information except for information (a) compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding; (b) information about another individual; (c) information obtained under a promise of confidentiality if disclosure would reveal the source of the information; and (d) information which, if disclosed, would be reasonably likely to endanger the life or physical safety of any individual. The Agency also will explain to a client any information that he or she does not understand. In addition, the Agency will allow a client to correct information which is inaccurate or incomplete. Corrections will be made by way of a new entry which is in addition to, but is not a replacement for, an older entry.

8. Security. The Agency will maintain security and confidentiality of HMIS information and is responsible for the actions of Agency Users and for their training and supervision. The Agency will follow all security policies established and provided in writing by the County. Among the steps Agency will take to maintain security and confidentiality are:

A. *Access.* The Agency will permit access to HMIS or information obtained from HMIS only to authorized Agency Users 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). The Agency will limit the access of such Users to only those records that are immediately relevant to their work assignments. The Agency will immediately notify County HMIS Administrator when User employment is terminated, so User access to HMIS may also be immediately terminated and account deactivated.

B. *User Policy.* Prior to permitting any user to access HMIS, the Agency will require the user to sign a ***HMIS User Policy, Code of Ethics and Responsibility Statement*** ("User Policy"), which is attached hereto as Appendix G and incorporated herein by this reference and which may be amended from time to time by the County. The Agency will comply with and enforce the User Policy and will inform the County immediately in writing of any breaches of the User Policy.

C. *Public Key Infrastructure (PKI).* PKI enables users of an unsecured network, like the Internet, to securely and privately exchange data through use of a cryptographic key pair, commonly called certificates. The certificates, or keys, will be issued by the County, and be distributed and attached to authorized Agency computers before access is granted.

D. *Computers.* Security for data maintained in Snohomish County's HMIS depends on a secure computing environment. The computer security requirements contained in this subsection are adapted from relevant provisions of the HUD Final Notice. The Agency is expected to directly consult the HUD Final Notice for complete documentation of HUD's standards relating to HMIS. The Agency will allow access to HMIS only from computers which are:

(i) physically present on Agency's premises; and owned by Agency, or approved by Agency for the purpose of accessing and working with HMIS;

(ii) protected from viruses by commercially available virus protection software (A) that includes, at a minimum, automated scanning of files as they are accessed by users on the system on which the HMIS application is housed and (B) with virus definitions that are regularly updated from the software vendor;

(iii) protected with a secure software or hardware firewall between, at least, the workstation and any systems (including the internet and other computer networks) located outside of the Agency;

(iv) maintained to ensure 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;

(v) accessed through web browsers with 128-bit encryption (e.g., Google Chrome, version 59). 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 Snohomish County's HMIS; the end-user is expected to physically enter the password each time he or she logs on to the system; and

(vi) 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 usable by unauthorized individuals. These steps should minimally include (a) logging off the data entry system, (b) physically locking the computer in a secure area, or (c) shutting down the computer entirely.

E. *User Authentication.* The Agency will permit access to HMIS only with use of a user authentication system consisting of a username and a 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, numbers and symbols. Passwords shall not be, or include, the username, the HMIS vendor's name, or the HMIS name or consist entirely of any word found in the common dictionary or any of the foregoing spelled backwards.

The use of default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access (e.g., usernames and passwords) may not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time. Passwords and user names shall be consistent with guidelines issued from time to time by HUD and the County.

F. *Hard Copies.* The Agency must secure any paper or other hard copy containing identifying information that is generated either by or for HMIS, including but not limited to reports, data entry forms and signed consent forms. Any paper or other hard copy generated by or for HMIS that contains identifying information must be supervised at all times when it is in a public area. If Agency staff is not present, the information must be secured in areas that are not publicly accessible. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location.

G. *Training/Assistance.* The Agency will permit access to HMIS only after the authorized User receives appropriate confidentiality training, including that provided by the County. The 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. The Agency will participate in such training as is provided from time to time by the County. Representatives of the County will be reasonably available during the County's defined weekday business hours for technical assistance (i.e., troubleshooting and report generation).

H. *Records.* The Agency and the County will maintain records of any disclosures of identifying information either of them makes of HMIS information for a period of seven (7) years after such disclosure. On written request of a Client, the Agency and the County will provide an accounting of all such disclosures within the prior seven-year period. The County will have access to an audit trail from HMIS so as to produce an accounting of disclosures made from one Partner Agency to another Partner Agency by way of sharing of information from HMIS.

I. *Retention of paper copies of personally identifying information.* The Agency and the County may not retain paper copies of personally identifying information derived from HMIS longer than seven years after the last day the person is served by the Agency. Paper copies will be destroyed through the use of a paper shredder or through a contract with a shredding management company.

9. Information Entry Standards.

A. Information entered into HMIS by the Agency will be truthful, accurate, complete and timely to the best of Agency's knowledge.

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

C. The Agency will only enter information into the HMIS database with respect to individuals which it serves or intends to serve, including through referral.

D. The Agency will enter information into the HMIS database as soon as possible and no longer than 5 days after data collection. Delays in data entry cannot be such that it interferes with clients receiving services.

E. The Agency will not enter identified information into the HMIS database unless it has obtained the written consent to do so, in accordance with Section 4 hereof, of the Client whose personal information it is. The Agency will not mark identified information for sharing with other Partner Agencies unless it has obtained the written consent to do so, in accordance with Section 4 hereof, of the Client whose personal information it is.

F. The Agency will not alter or over-write information entered by another Agency, unless revised documentation has been received regarding the client's personally identifiable information, necessitating an update in the system (e.g. client provides full Social Security number).

10. Use of Snohomish County HMIS.

A. The Agency will not access in HMIS the identifying information for any individual for whom services are neither sought nor provided by the Agency. The Agency may access identifying information of the Clients it serves and may request, via writing addressed to the County's authorized officer shown on the signature page of this Agreement, access to statistical, non-identifying information on both the Clients it serves and the Clients served by other Partner Agencies.

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

C. The Agency and the County will report only non-identifying information in response to requests for information from HMIS.

D. The Agency will use the HMIS database for its legitimate business purposes only.

E. The 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, obscene, or confidential.

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

11. Proprietary Rights.

A. The Agency shall not give or share assigned passwords and access codes for HMIS with any other agency, business, or individual.

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

12. Limitation of Liability of Parties and Indemnification. No party to this Agreement shall assume any additional liability of any kind due to its execution of this Agreement or its participation in the HMIS system. 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 through participation in HMIS except for the acts and omissions of its own employees, volunteers, agents or contractors. The parties specifically agree that this Agreement is for the benefit of the parties only and creates no rights in any third party.

13. Limitation of Liability of County. The County and the Snohomish County HMIS shall not be held liable to any Partner Agency for any cessation, delay or interruption of services, nor for any malfunction of hardware, software or equipment.

14. Disclaimer of Warranties. The County makes no warranties, express or implied, including warranties of merchantability or fitness for a particular purpose, to any agency or any other person or entity as to the services of the HMIS system or as to any other matter.

15. Term of Agreement; Termination of Prior Agreement. This Agreement shall be effective upon its execution by both parties hereto [and, upon such execution, the Prior Agreement between the parties shall be terminated and of no further force or effect]. This Agreement shall terminate as provided in Section 16E hereof.

16. Additional Terms and Conditions.

A. The Agency will abide by such guidelines as are promulgated by HUD and the County from time to time regarding administration of the HMIS.

B. The Agency and the County 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, the Agency and the County agree to modify the terms of this Agreement so as to comply with applicable law.

C. Neither the County nor the Agency will transfer or assign any rights or obligations under this Agreement without the written consent of the other party.

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

E. This Agreement will be in force until terminated by either party. Either party may terminate this Agreement for any reason with twenty (20) days' prior 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 by the Agency of written security policies established by the County.

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

G. Copies of Agency data will be provided to the Agency upon written request upon 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 by the County of a written request by the Agency for data copies.

AGENCY NAME

By _____ Date _____
(signature)

_____
Name and Title of Authorized Officer

Street Address:
Mailing Address:
Telephone:
Facsimile:
Email:

SNOHOMISH COUNTY

By _____ Date _____
Mary Jane Brell Vujovic, Director
Human Services Department

Street Address: 3000 Rockefeller Avenue, M/S 305
Everett, Washington 98201-4046
Mailing Address: Same as above
Telephone: (425) 388-7200
Facsimile: (425) 259-1444
Email: MaryJane.Vujovic@co.snohomish.wa.us

Reviewed and approved
Pursuant to SCC 3.04.016 by:

_____
Viggo Forde, Director Date
Information Services

Approved as to form only:

_____
Deputy Prosecuting Attorney Date

Appendix C

HMIS Forms Overview

2019 Security Changes: Changes have been made to the HMIS Consent and Release of Information forms and Snohomish County's HMIS in ClientTrack. Those changes were made to reduce duplication of client records and agency efforts, increase coordination and data sharing, and to allow for streamlined referral processes around Coordinated Entry.

By signing the new form, clients consent to their personal information being **entered and shared** with HMIS Partner Agencies. There are no longer different options for sharing information; if data is entered, it is also able to be shared. If a client refuses consent, then they will be entered anonymously per the local HMIS Data Entry Manual. Anonymous records will be shared as well.

By signing the new form, unaccompanied youth aged 13 or older **can consent** to their personally identifiable information being entered into the database. This complies with RCW 43.185C.180.

Existing clients will need to be presented with the new form at their next appointment, then have their **information release codes updated** in the database. Case managers do not need to schedule special appointments to have the new forms signed, but should get them signed at the next regularly scheduled appointment or annual assessment/review, whichever comes first.

There is a **new yes/no question** on all intake forms for heads of households aged 13 and older, and family members aged 18 and older: "Has the client signed the 2019 Release of Information?" This question will also need to be answered as codes are updated for existing clients.

The new consent and release form **expires seven (7) years** from the last recorded HMIS activity. We will change the default dates to reflect that change in terms, but you will need to update the expiration date manually as existing clients sign new forms and their numbers are updated.

Persons being served by Domestic Violence agencies, others currently fleeing or in danger from a domestic violence, dating violence, sexual assault, or stalking situation, or those who are being served in a program that requires the disclosure of HIV/AIDS status **must not sign** the form. They must all be entered anonymously.

All persons aged 18 or older (or unaccompanied youth aged 13 or older) must **sign their own form**. Parents/guardians can sign for children under 18 in their household being served by the program.

FORMS

HMIS Client Privacy Rights: About Your Information

Explanation: The Client Privacy Rights document is meant to provide additional information to clients about HMIS. It explains who sees their information, what their rights are, what the risks are, and the choices they have.

Requirements:
Pursuant to the HUD Final Notice, each Agency must prominently display the HMIS Client Privacy Rights at each intake desk (or comparable location).

HMIS Informed Consent and Release of Information Authorization (IC-ROI)

Explanation: The Informed Consent and Release of Information Authorization gathers a client's consent to having Personal Identifiable Information (PII) entered into the HMIS.

Requirements:
Consent must be provided by the household before any PII is entered and shared in HMIS. Originals of the IC-ROI must be kept by the agency for seven (7) years after the date of signature.

Each adult in the household must sign their own IC-ROI. A parent or guardian can sign for their dependents. If an adult client has been declared legally incompetent, the court appointed guardian must sign and provide a copy of the order of appointment. If someone is signing in another capacity (including a person with a power of attorney), obtain a copy of the legal authority to act.

The Snohomish County HMIS web page is updated to provide clients with a list of all partner agencies who may have access to their PII.

Client Revocation of HMIS Consent

Explanation: A Client may withdraw or revoke their consent for the entry of PII by signing the Revocation of HMIS Consent form located on the HMIS website at https://snohomishcountywa.gov/852/HMIS-Documents.

Requirements: If a client revokes their consent, the Agency is responsible for immediately contacting the HMIS administrator to ensure that PII is removed from the HMIS.

Appendix D

HMIS Client Privacy Rights: About Your Information

HMIS CONSENT AND RELEASE OF SHARING AUTHORIZATION	• Information you provide to this agency will be entered into the Snohomish County HMIS computer system, unless you tell them you do not want it entered. • If you provide consent, your record will be entered into HMIS and shared with all HMIS Partners. Your record includes your Name, Date of Birth, Social Security Number, Ethnicity, Race, Gender, and whether you have served in the military or have a disabling condition. Your record also includes program enrollments, assessments, housing information, use of crisis services, case notes, services provided by Partner Agencies, basic medical, mental health, substance use, employment, income, insurance, and benefit information. This information will be kept in the HMIS database for seven (7) years. • You will receive the same services whether or not you allow your personal information to be entered into the HMIS and shared with other agencies through the HMIS Informed Consent and Release of Information Authorization form. • Your personal information that is collected by this Agency or in the HMIS will not be shared with any other government agencies except as required by law. • Your data is protected by legal agreements signed by users of the HMIS and by electronic encryption of your personal information. • Information collected in HMIS is used to improve services to clients. • You can contact Snohomish County at the number below if: o You have questions about the information collected in the HMIS and your rights regarding that information. o In the event of an injury to you related to the collection of information in the HMIS. Although careful measures are taken to protect the personal information entered into the HMIS, it may be possible that a person could access your information and use that information to locate you, commit identity theft, or learn about sensitive personal information entered into the HMIS.
YOUR RIGHTS AND CHOICES	• You have the right to refuse to provide personal information, or to stop this agency from entering your personal information into the HMIS system. • You have the right to change your mind about what personal information about you this agency has entered in the HMIS. You must notify this Agency in writing if you change your mind. • Your records are protected under Federal and State Confidentiality Regulations (42 CFR, Part 2, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 CRF, 160 & 164) and cannot be disclosed without your written consent unless otherwise provided for in the regulations.

<table>
<tr><td>WHO
CAN SEE MY
INFORMATION?</td><td colspan="2">

The following agencies will have access to a limited amount of your information. You may request a list of the information that they have access to:

Washington State Dept. of Commerce, as the administrator of the Washington State HMIS.
A few staff members of the Research Division at DSHS who have signed confidentiality agreements.

Additionally, in limited circumstances the following agencies will be conducting research:

Snohomish County Human Services Department
HMIS Partner Agencies found at https://snohomishcountywa.gov/756/Homeless-Management-Information-System.

</td></tr>
<tr><td>CONTACT
INFORMATION</td><td>Snohomish County, Data Security Officer
Office of Housing and Community Services
3000 Rockefeller Ave, M/S 305, Everett, WA 98201
425-388-3270
https://snohomishcountywa.gov/</td><td>[Agency Name]
[Agency Address]
[Agency phone]
[Agency email]
[Agency website]</td></tr>
</table>

Revised January 2019

Appendix E

HMIS Informed Consent and Release of Information Authorization

This Agency participates in the Snohomish County Homeless Management Information System (HMIS), which is a database that is used to collect information, over time, about the characteristics and service needs of men, women, and children experiencing homelessness or who are at-risk of homelessness. This information is gathered and stored to improve access to services while meeting requirements of funders such as the U.S. Department of Housing and Urban Development (HUD).

To provide the most effective services in moving people from homelessness to permanent housing, we need an accurate count of all people experiencing homelessness in Snohomish County. To make sure that clients are not counted twice if services are provided by more than one agency, and to facilitate care coordination and housing placement services, we need to collect some personal information. Your information will be stored in our database for seven (7) years. This information will be shared with Partner Agencies for the purposes of providing housing placement services. A current list of these HMIS Partner Agencies is available online at https://snohomishcountywa.gov/756/Homeless-Management-Information-System. If you have questions about data collection or your rights regarding your personal information, please contact the HMIS System Administrator at 425-388-3270.

By signing this form, I give this Agency permission to share (verbally, or through the HMIS, mail, fax, or by hand) information collected about me and any dependents listed on the back of this form with HMIS Partner Agencies, for the purposes of care coordination and housing placement or retention services, including:

- name, date of birth, gender, race, ethnicity, social security number, phone number, address
- program enrollments and assessments
- housing information
- use of crisis services, hospitals, and jails
- case notes and services provided by Partner Agencies
- basic medical, mental health, substance use and daily living information
- employment, income, insurance, and benefit information

By signing this, I certify I understand that:

- The data I provide will be combined with data from the Department of Social and Health Services (DSHS) for further analysis. My name and other identifying information will not be included in any reports or publications. Only a limited number of staff members in the research division who have signed confidentiality agreements will be able to see this information, and my information will not be used to determine eligibility for DSHS programs. Snohomish County and Washington State HMIS system administrators have full access to all information in the HMIS, including Department of Commerce staff, designated agency system administrators, and applicable HMIS software vendors.

- My decision to participate in the HMIS will not affect the quality or quantity of services I am eligible to receive from this agency, and will not be used to deny outreach, assistance, shelter, or housing. However, if I do choose to participate, services in the region may improve if we have

accurate information about homeless individuals and the services they need. Furthermore, some funders **may** require that I consent to my information be supplied in the HMIS in order for me to receive services from that funding source.

- The Snohomish County HMIS guards this information with strict security policies to protect my privacy, using a computer system that is highly secure and uses up-to-date protection features such as data encryption, passwords, and identity checks required for each system user. There may be a risk of a security breach, whereby someone might obtain and use your information inappropriately. If you ever suspect that your data in the HMIS has been misused, and/or to report possible injury arising from the use of such data, immediately contact the HMIS System Administrator at 425-388-3270.

- The purpose of sharing this information with HMIS Partner Agencies is to help with care coordination, improve the services I receive, and allow HMIS Partner Agencies to access information about me quickly if needed.

- I am entitled to a copy of this release and sharing form.

- I may revoke this sharing permission at any time by delivering or mailing a written statement canceling my consent and release of information to this Agency. Revoking my consent/release will not change anything for those people or agencies that had previously received my information while my consent/release was in effect.

- I understand that additional Partner Agencies may join the Snohomish County HMIS and will also have access to this information at that time. I understand that, upon my request, this Agency must provide me with a list of current HMIS Partner Agencies before I sign this release and information sharing form, and must allow me to view the updated list of agencies so long as my release/sharing permission remains in effect.

- I understand that my records are protected under Federal and State Confidentiality Regulations (42 CFR, Part 2, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 CFR, 160 & 164) and cannot be disclosed without my written consent unless otherwise provided for in the regulations.

- I understand that my HMIS information may be shared with additional agencies to coordinate referral and placement for housing as well as care coordination.

- This Consent and Release of Information will expire seven (7) years from my last HMIS-recorded activity.

- I have reviewed a copy of the Snohomish County HMIS Client Privacy Rights posted at this Agency.

Note: We are not required to agree to additional restrictions that you request beyond those listed here, but, if we do agree to additional restrictions (that you request in writing), then they are binding on this Agency and on the Snohomish County HMIS.

IMPORTANT: Do not enter personally identifying information into HMIS for clients who are: 1) in DV agencies; 2) currently fleeing or in danger from a domestic violence, dating violence, sexual assault, or stalking situation; or 3) being served in a program that requires disclosure of HIV/AIDS status (i.e., HOPWA). *If this applies to you, STOP – do not sign this form.*

Dependent children under 18 in household, if any (please print first and last name):

_____ _____

_____ _____

_____ _____

CLIENT SIGNATURE (PARENT/GUARDIAN) **DATE**

_____ _____

CLIENT NAME (PRINTED) **STAFF NAME (PRINTED)**

Appendix F

Client Revocation of HMIS Consent

I revoke my permission for _____ (agency) **to have or enter my identified personal information** in the Snohomish County HMIS computer system. This also means that **I do not give permission to this agency to share** any of my information in the Snohomish County HMIS computer system.

☐ No personal information may remain:

In the System:	Not in the System:
(no identified information)	• Gender (if provided) • Name (if provided) • Social Security Number (if provided) • Last Permanent Address (if provided) • Phone Number (if provided) • Date of Birth (if provided)

I understand that the same services will be available to me whether or not I allow this agency to enter my identified personal information into the Snohomish County HMIS.

Client or Guardian Signature	Date	Relationship to Client
Print Name		
Agency Witness Signature	Date	
Print Name		

Appendix G

HMIS User Policy, Code of Ethics, and Responsibility Statement

For: From:

User Name (*print name*) Agency *(print or type name)*

User Agency Email User Date of Hire

1. USER POLICY

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

b. It is a client's decision about which information, if any, is entered into HMIS and whether that information is to be shared with any Partner Agencies. Prior to obtaining the client's signature, User shall review the ***HMIS Informed Consent and Release of Information Form*** with the client in a manner to ensure that the client fully understands the information (e.g., securing a translator if necessary). The ***HMIS Informed Consent and Release of Information Form*** must be signed by the client before any identifiable client information is designated in HMIS for sharing with any Partner Agencies.

2. USER CODE OF ETHICS

a. Users must be prepared to answer client questions regarding HMIS.

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

c. Users must allow a client to change his or her information sharing preferences at the client's request.

d. Users must not decline services to a client or potential client if that person refuses to allow entry of information into HMIS or to share their personal information with other agencies via HMIS.

e. The User has primary responsibility for information entered by the User. Information entered into HMIS by a User must be truthful, accurate, complete and timely to the best of User's knowledge.

f. Users will not solicit from or enter information about clients into HMIS unless the information is required for a legitimate business purpose such as to provide services to the client.

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

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

i. Users must permit clients to file a written complaint regarding the use or treatment of their information within HMIS. Clients may file a written complaint with either the Agency or with the Snohomish County Human Services Department at 3000 Rockefeller Avenue, M/S 305, Everett, WA 98201. Clients may not be retaliated against for filing a complaint.

3. USER RESPONSIBILITY

Your username and password give you access to the HMIS system.

Initial each item below to indicate your understanding and acceptance of the proper use of your username and password. Failure to uphold the confidentiality standards set forth below is grounds for immediate termination from HMIS database access, and may result in disciplinary action from the Partner Agency as defined in the Partner Agency's personnel policies.

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

_____ a. My username and password are for my use only and will not be shared with anyone.

_____ b. I will read and abide by the ***Snohomish County HMIS Client Privacy Rights***, ensuring clients understand their rights.

_____ c. I will not use the browser capacity to remember passwords: I will enter the password each time I log on to the HMIS.

_____ d. I will take reasonable means to keep my password physically secure.

_____ e. I will only view, obtain, disclose, or use the database information that is necessary to perform my job.

_____ f. I understand that the only individuals who may directly access HMIS client information are authorized users, and I will take the following steps to prevent casual observers from seeing or hearing HMIS client information.

_____ (i) I will log off the HMIS before leaving my work area, or make sure that the HMIS database has "timed out" before leaving my work area.

_____ (ii) I will not leave unattended any computer that has HMIS "open and running."

_____ (iii) I will not use the HMIS system from an unauthorized computer (e.g., home computer) or unauthorized network (e.g., public Wi-Fi).

_____ (iv) I will keep my computer monitor positioned so that persons not authorized to use HMIS cannot view it.

_____ (v) I will store hard copies of HMIS information in a secure file and will not leave such hard copy information unattended or in public view on my desk, or on a photocopier, printer or fax machine.

_____ (vi) I will properly destroy paper copies of HMIS information when they are no longer needed unless they are required to be retained in accordance with applicable law.

_____ (vii) I will not discuss HMIS confidential client information with staff, clients, or client family members in a public area.

_____ (viii) I will not discuss HMIS confidential client information on the telephone in any areas where the public might overhear my conversation.

_____ (ix) I will not leave messages on my agency's voicemail system that contains HMIS confidential client information.

_____ (x) I will keep voicemail volume low, ensuring HMIS confidential information left by callers is not overheard by the public or unauthorized persons.

_____ g. I understand that a failure to follow these security steps appropriately may result in a breach of client HMIS confidentiality and HMIS security. If such a breach occurs, my access to HMIS may be terminated and I may be subject to further disciplinary action as defined in the Partner Agency's personnel policy.

_____ h. If I notice or suspect a security breach, I will immediately notify the Director of my Agency and the Snohomish County HMIS Security Officer.

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

_____ _____ _____

HMIS User Signature Date HMIS User Name (*please print*)

_____ _____ _____

Agency Director Signature Date Agency Director Name (*please print*)

Appendix H

Data Quality Plan

A. Overview

In order for the Continuum to have reliable data for analysis and reporting, the County and Partnering Agencies must develop a document that outlines program and system-level expectations for data collection and entry into the HMIS. This document, called a Data Quality Plan, will be used as the basis for developing goals for achieving quality data. To achieve these goals, we must develop, implement, and monitor a data quality plan that outlines goals, tasks, task leads, and timelines and regularly assesses the progress of both programs and the system as a whole towards meeting the overall data quality benchmarks.

B. Components

At a minimum, the data quality plan will include the following:

1. Timeliness: entering data in a timely manner can reduce human error that occurs when too much time has elapsed between the data collection and the data entry. The individual doing the data entry may be relying on handwritten notes or their own recall of a case management session, a service transaction, or a program exit date; therefore, the sooner the data is entered, the better chance the data will be correct. Timely data entry also ensures that the data is accessible when it is needed.
    a. Benchmark –
        i. Coordinated Entry, Enrollment – 1 calendar day
        ii. Coordinated Entry , Navigator Assessment – 5 calendar days
        iii. Emergency Shelter – 5 calendar days
        iv. Homelessness Prevention – 5 calendar days
        v. Permanent Housing Other – 5 calendar days
        vi. Permanent Supportive Housing – 5 calendar days
        vii. Rapid Rehousing – 5 calendar days
        viii. Services only – 5 calendar days
        ix. Street Outreach – 5 calendar days
        x. Transitional Housing – 5 calendar days

    b. Method for obtaining and tracking this information: Average length of time between the program entry date and the date the enrollment record was created and the average length of time between the exit date and the date the exit assessment was created.

2. Completeness

   a. General: partially complete or missing data (e.g. missing the birth date, disability or veteran status) can negatively affect the ability to provide comprehensive analysis in reporting. Incompleteness also affects our Continuum's ability to sift duplicate client level data.

      i. For the system-wide benchmarks, see table below (percentages rounded):

Data Element	**Records that are complete**	**Records where value is unknown benchmark**	**Records where value is refused benchmark**	**Records where value was not collected benchmark**	**Records where value is missing benchmark**
Name Quality	95%	0%	4.1%	0%	0.9%
SSN Quality	72.6%	8.9%	7.1%	11.4%	0%
Date of Birth Quality	100%	0%	0%	0%	0%
Relationship to Head of Household	100%	0%	0%	0%	0%
Race	98.9%	0.3%	0.8%	0%	0%
Ethnicity	99.4%	0.2%	0.4%	0%	0%
Gender	99.6%	0.1%	0.1%	0%	0.2%
Client Location	100%	0%	0%	0%	0%
Veteran Status	99.5%	0.1%	0.1%	0%	0.3%
Disabling Condition	98.9%	0.3%	0.2%	0%	0.6%
Project Start Date	100%	0%	0%	0%	0%
Project Exit Date	100%	0%	0%	0%	0%
Exit Destination	98.2%	0.4%	0.3%	0.6%	0.5%
Prior Living Situation	98.9%	0.1%	0.1%	0%	0.9%
From the Streets or Emergency Shelter	81%	0%	0%	0%	19%
Number of Times Homeless	93.9%	0.5%	0.1%	0.7%	4.8%
Length of Stay Prior Residence	98.7%	0.3%	0.1%	0%	0.9%
Homeless Start Date	88.6%	0%	0%	0%	11.4%
Number of Months Homeless	91.6%	0.6%	0.1%	0.2%	7.5%

ii. For benchmarks by program type, see attached data quality monitoring plan.

b. Bed utilization rates: looking at a program's bed utilization rate or the number of beds occupied as a percentage of the entire bed inventory, is an excellent barometer of data quality. It is difficult to measure data quality if the utilization rate is too low (below 65%) or too high (above 105%). Low utilization rates could indicate that the residential facility was not at or near capacity, but it could also mean the HMIS data is not being entered for every client served. High utilization rates could mean the bed provider was over capacity, but it could also mean the program has not properly exited clients from the system.

3. Accuracy
    a. General: the purpose of accuracy is to ensure that the data in HMIS is the best possible representation of reality as it relates to homeless people and the programs that serve them. All data entered in HMIS shall reflect information provided by the client, as documented by agency staff, or otherwise updated by the client and documented for reference. Recording inaccurate information is strictly prohibited.
    b. Starting a new project within HMIS: Agencies are expected to inform Snohomish County HMIS Admin staff one (1) month prior to the start of any new project through use of the online HMIS Project Form found on the Snohomish County HMIS Documents web page to ensure proper project set-up.
    c. Ending a project within HMIS: Agencies are expected to inform their contract managers and Snohomish County HMIS Admin staff at least one (1) month prior to a project ending.
    d. Consistency: consistency benchmarks will include developing companion documents that describe the enrollment and assessment forms, data entry methods, wording of questions, and enrollment and data entry training schedules. These documents will be cross-referenced with the most current HUD HMIS Data Standards.

4. Data Quality Review: data quality review will be done on a bi-monthly basis.

    Additionally, other data quality monitoring and reporting occurs throughout the year.

    a. The Longitudinal Systems Analysis (LSA) report is an annual report submitted to HUD. For this reporting process, agency staff are required to submit inventory updates at a minimum of four (4) times a year to Snohomish County HMIS Admins to make sure the inventory is correct for the dates of: January 31, April 30, July 31, and October 31. Any data issues identified by the County including but not limited to client data, performance outcomes, and inventory data for the LSA must be addressed per the data standards.
    b. Access to Data Quality Reports: By the 15 of every other month, HMIS Admin staff will make data quality reports available for the purposes of facilitating compliance review by participating agencies and any necessary CoC Data Committee. When the 15th falls on a weekend or holiday, these reports shall be made available on the next business day.

        Data Correction: participating agencies will have 10 business days to correct data issues identified in the Data Quality reports. HMIS Admin staff will then make available revised data quality reports for posting to the HMIS website by the 30th of every other month.

5. Other components
    a. Access to the Data Quality Plan: the data quality plan will be posted to the Snohomish County HMIS web page.
    b. Data Quality Roles and Responsibilities: Each agency is expected to outline and update the roles and responsibilities of entering, maintaining, and correcting their agency's data. Agencies will do this through the Snohomish County Data Quality Roles and Responsibilities worksheet. This worksheet will be included in each Agency's bi-monthly Data Quality Review for review or revisions as necessary. (See Appendix J)
    c. Bi-monthly Data Quality Review: HMIS Admin staff will review participating agency data quality reports for compliance with the data quality benchmarks, working with participating agencies to identify training needs to improve data quality.
    d. The HMIS Lead Agency will develop a public-facing Tableau dashboard to display agency aggregate data quality on the Snohomish County HMIS Tableau website. Continuum of Care Review: HMIS Admin staff will provide brief updates on progress related to data quality benchmarks.
    e. Encouragements: HMIS Admin staff will highlight organizations and projects exceeding data quality benchmarks at HMIS User Group Meetings.
    f. Enforcement: For agencies that fail to meet data quality benchmarks, HMIS Admin staff will create a Data Quality Improvement Plan using current guidance from the HUD HMIS Lead Series.

Appendix I

Monitoring of Data and HMIS Security

A. Overview

Snohomish County HMIS Lead Agency will complete an annual review to ensure Agencies are following all security, privacy, and data technical standards. Monitoring is a benefit to Agencies, Clients and the Public as it ensures required security and privacy measures have been implemented are still functioning as intended. Potential issues may be identified and resolved with the Agency as an active partner. Conversely, a high performing agency may be recognized for its efforts. Annual HMIS monitoring should be completed within 45 days from the monitoring opening conference date unless a different schedule is agreed upon by the agency and the county.

Data will be reviewed by the HMIS Lead Agency for accuracy, completeness, and timeliness on a bi-monthly basis. Client data in HMIS is expected always to be completely accurate. Inaccurate or missing data will be flagged for correction, regardless of percentage. Completeness compliance includes no missing (null) data for required program elements. Responses that are unknown or refused shall not exceed the allowed percentages in any given month. Housing programs shall stay within the allowed utilization rates. The average timeliness rate in any given month shall be with standard timeframe of five days for non-Coordinated Entry programs and one day for Coordinated Entry Enrollments.

B. Administrative Data Monitoring – Remote or Site Visit

The HMIS Administrator shall review Agency HMIS and Coordinated Entry data input for timeliness, completeness, correctness, duplication, and outcomes on a bi-monthly basis as noted above. It is expected that accuracy remain at no less than 100% for all client and transactional data at all agencies. The HMIS Administrator reserves the right to compare agency paper files at agency site against HMIS and Coordinated Entry data in the database to confirm accuracy and completeness. Site visits will be scheduled with Agency Leadership in advance in order to reduce administrative burden on Agency staff.

C. Data Entry Compliance

Given that an expectation exists that 100% of the reviewed data elements per program are correct to meet this Continuum of Care's standards, agencies must correct all errors identified by the reviewer. Technical assistance will be provided by the HMIS Lead to assist the agency in reaching and maintaining compliance with this standard.

Data produced from HMIS is critical to meet the reporting and compliance requirements of HUD, Funders, individual agencies, and the Continuum of Care as a whole. When data quality benchmarks are met, reporting will be more reliable and can be used to evaluate the delivery of services, program design and system effectiveness.

D. Hardware Security Monitoring – Site Visit

All networks, computers or similar devices used to access the HMIS platform must be owned and maintained by the Agency's Information Technology Department. These Agency networks and devices used to access HMIS must have virus protection and a firewall installed. Firewall must be placed between any device and the internet connection. Virus definitions and firewall must be regularly updated by the Agency. HMIS Lead Agency will confirm that participating Agency has virus protection and firewall installed at annual security review.

Device screens must not be visible to staff, Users, Clients, and the Public who do not have written authorization and a clear purpose to view the data presented on the screen. HMIS Lead Agency will confirm screens are hidden from view by placement or a privacy film has been installed at annual security review.

Exported electronic personally identifiable data shall remain on a secured network drive and remain inaccessible except to those who are authorized and have a purpose to view. This will be confirmed at annual User interview.

Personally Identifiable Information which has been printed from or for the HMIS shall remain secured and inaccessible except to those who are authorized and have a purpose to view. This will be confirmed at annual User interview.

E. User Interviews During Monitoring

On an annual basis, a sampling of Users will be interviewed to ensure compliance with existing security, privacy, and technical standards. Users will review and sign an updated HMIS User Policy, Code of Ethics, and Responsibility.

F. Monitoring Follow-Up

The HMIS Administrator will follow-up on the monitoring results within 5 business days to ensure that any data flagged for correction has been updated and any program improvements have been implemented. Technical assistance will continue to be provided as needed or requested by Agency to ensure success with compliance.

G. Non-Compliance with Security or Privacy Measures

Any end User found in violation of security protocols in the HMIS Policies and Procedures will be coached and/or sanctioned accordingly. Sanctions may include permanent revocation of system access privileges by HMIS Administrator and Agency action.

H. Agency Non-Compliance with HMIS Monitoring

If an Agency that fails to implement a corrective action plan and/or intentionally refuses to come into compliance, the HMIS Lead shall elect to take one or all of the following remedial actions or sanctions.

1. Develop an action plan to bring affected data and programs into compliance.
2. Suspend Agency access to HMIS.
3. Terminate Agency access to HMIS.
4. Impose other legally available remedies.

HMIS Annual Security Monitoring Checklist

Agency Name: _____Date: _____

Visit Completed By: _____Title: _____

Requirement	Assessment	Notes/Comments
An HMIS Privacy Statement is visibly posted at each HMIS workstation.	☐ Yes ☐ No	
Each User is using the most current versions of the Client Consent and Release forms.	☐ Yes ☐ No	
Each HMIS workstation computer is in a secure location where only authorized Users have access.	☐ Yes ☐ No	
Each HMIS workstation computer is password protected and locked when not in use.	☐ Yes ☐ No	
Users' login credentials are kept secure from unauthorized use.	☐ Yes ☐ No	
Non-authorized persons are unable to view any HMIS workstation computer monitor.	☐ Yes ☐ No	
Each HMIS workstation computer has antivirus software installed with updated definitions.	☐ Yes ☐ No	

Agency network has a firewall in place with up-to-date security settings.	☐ Yes ☐ No	
Users are accessing HMIS only through an Agency maintained network, not public wifi.	☐ Yes ☐ No	
Client protected personal information has not been electronically stored or transmitted in any manner (hard drive, email, flash drive, etc).	☐ Yes ☐ No	
Hard copies of client protected personal information are stored in a physically secure location.	☐ Yes ☐ No	
Each user signed a current HMIS User Policy, Code of Ethics, and Responsibility statement.	☐ Yes ☐ No	
Users were given the opportunity at interview to discuss any security concerns	☐ Yes ☐ No	
Each User with access to HMIS has a continued need to access HMIS.	☐ Yes ☐ No	

Reviewed By: _____ Title: _____

Reviewed By: _____ Title: _____

Appendix J

Snohomish County Data Quality: Roles and Responsibilities Worksheet

Agency:_____

Completed/Updated Date:_____

Background

The different roles associated with Homeless Management Information System (HMIS) data collection, operations, policy and procedure development, data quality (DQ) monitoring, and reporting can all play a meaningful part in upholding a Continuum of Care (CoC)'s DQ Management Program. This worksheet is intended for Snohomish County HMIS Admins and Partner Agencies to have a clear expectation of who is responsible for data entry, correcting data, and communicating needs to the HMIS Admin.

Data Collection and Entry

Action	Responsible individual	Responsible individual's supervisor
Collect enrollment and assessment data from clients		
Enter enrollment assessment data in HMIS		
Update HMIS to reflect changes in income, benefits, etc.		
Collect exit assessment data from clients (including exit destination)		
Enter exit assessment data in HMIS		
Secure paper forms according to privacy and confidentiality standards		

Maintain workstation security		

Bi-Monthly DQ Reports

Action	Responsible individual	Responsible individual's supervisor
Receive Bi-Monthly DQ Reports for timeliness, completeness, accuracy, and consistency		
Correct low-quality data at the program level based on Bi-Monthly DQ Reports for timeliness, completeness, accuracy, and consistency		
Participate in the HMIS User Group Meetings		

Monitoring and Reporting

Action	Responsible individual	Responsible individual's supervisor
Monitor DQ for completeness (client and program)		
Monitor DQ for timeliness		
Monitor DQ for accuracy		
Monitor DQ for consistency		
Review analyzed project-level and system-level trends in DQ performance		
Assist HMIS Admin in reviewing Agency's data for HUD reports prior to submission		

Manage program-level reporting requirements by service and/or funder		

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement, hereinafter referred to as the "Agreement," is entered into by and between Snohomish County, a political subdivision of the State of Washington, on behalf of its Human Services Department, hereinafter referred to as "County," and (Agency Name)**,** hereinafter referred to as "Agency."

I. PURPOSE

A. The Parties wish to enter into this Agreement to comply with the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended (collectively, "**HIPAA**"), together with the Health Information Technology for Economic and Clinical Health Act (HITECH Act).

B. It is the purpose of this Agreement to establish requirements that may be incorporated by reference into subsequent contracts between the County and the Agency for social and health services funded in whole or in part by or through the County that may involve Agency creating, receiving, maintaining, or transmitting PHI, as defined below in which the Agency may be considered a "Business Associate" of the County under HIPAA. Any reference to Business Associate in the Agreement includes Business Associate's employees, agents, officers, subcontractors, third party contractors, volunteers or directors. This document has no independent force or effect.

II. DEFINITIONS

A. "Authorized User(s)" means an individual or individuals with an authorized business requirement to access Confidential Information.

B. "Breach" means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under HIPAA, which comprises the security or privacy of the PHI, with the exclusions and exceptions listed in 45 CFR. § 164.402.

C. "CFR." shall mean the Code of Federal Regulations. All references in this Agreement or any Contract to the CFR shall include any successor, amended, or replacement regulation.

D. "Confidential Information" means information that is exempt from disclosure to the public or other unauthorized persons under Chapter 42.56 RCW or other federal or state laws. Confidential Information includes, but is not limited to, Personal Information.

E. "Contract" means any agreement between the County and the Agency that incorporates this Agreement by reference.

F. "Disclose" and "disclosure" mean, with respect to Protected Health Information, the release, transfer, provision of access to, or divulging in any other manner of Protected Health Information outside Agency's internal operations or to other than its employees.

G. “Electronic Protected Health Information (EPHI)” means Protected Health Information that is transmitted by electronic media or maintained in any medium described in the definition of electronic media at 45 CFR. § 160.103.

H. “Hardened Password” means a string of at least eight (8) characters containing at least one (1) alphabetic character, at least one (1) number and at least one (1) special character such as an asterisk, ampersand or exclamation point.

I. “HIPAA Rules” means the Privacy, Security, Breach, Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

J. “Individual” means the person who is the subject of Protected Health Information and shall include a person who qualifies as a personal representative in accordance with 45 CFR. § 164.502(g).

K. “Minimum Necessary” means the least amount of PHI necessary to accomplish the purpose for which the PHI is needed.

L. “Personally Identifiable Information” (PII) shall mean information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

M. “Personal Information” (PI) means information identifiable to any person, including, but not limited to, information that relates to a person’s name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, driver license numbers, other identifying numbers, and any financial identifiers.

N. “Protected Health Information” (PHI) is information created or received that relates to the provision of health care to an individual; the past, present, or future physical or mental health or condition of an individual; or past, present or future payment for provision of health care to an individual. 45 CFR 160 and 14. PHI includes demographic information that identifies the individual or about which there is reasonable basis to believe, can be used to identify the individual. 45 CFR 160.103. PHI is information transmitted, maintained, or stored in any form or medium. 45 CFR 164.501. PHI does not include education records covered by the Family Educational Right and Privacy Act, as amended, 20 USCA 1232g(a)(4)(b)(iv).

O. "RCW" means the Revised Code of Washington. All references in this Agreement to RCW chapters or sections shall include any successor, amended, or replacement statute. Pertinent RCW chapters can be accessed at http://slc.leg.wa.gov/.

P. “Required by law” means a mandate contained in law that compels an entity to make a Use or Disclosure of Protected Health Information that is enforceable in a court of law. “Required by law” includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury or any administrative body authorized to require

the production of information; a civil or an authorized investigative demand; statutes or regulations that require the production of information.

Q. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

R. "Unique User ID" means a string of characters that identifies a specific user and that, in conjunction with a Hardened Password, passphrase or other mechanism, authenticates a user to an information system.

S. "Use" or "uses" mean, with respect to PHI, the sharing, employment, application, utilization, examination or analysis of such information within Agency's internal operations.

T. Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms are defined in the HIPAA privacy regulations.

III. OBLIGATIONS OF AGENCY

A. Use and Disclosure. The Agency shall not use or further disclose PHI other than as permitted or required by any Contract or as required by law.

B. Appropriate Safeguards. The Agency shall use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement.

C. Agency Agreement on Nondisclosure of Confidential Information. Pursuant to RCW 71A.124.070, the Agency shall ensure each employee who has access to Confidential Information sign the "Agency Agreement on Nondisclosure of Confidential Information" form (Nondisclosure Form), included with this Agreement as Attachment 1.

1. The Agency must have the Nondisclosure Form signed annually and maintained on file for a minimum of six (6) years.

2. The Agency shall have the form available for County review upon request.

3. This Nondisclosure Form requirement shall be included in all subcontracts

D. Mitigation. The Agency shall mitigate, to the extent practicable, any harmful effect that is known to Agency of a use or disclosure of PHI by Agency in violation of the requirements of this Agreement.

E. Reporting Unauthorized Use or Disclosure. The Agency shall report to the County within five (5) business days any use or disclosure of PHI not provided for by this Agreement of which it becomes aware.

F. Use of Agents and Subagencies. The Agency shall require that each of its agents and subagencies to whom it provides PHI received from, or created or received by Agency on behalf of the County agree in writing to the same restrictions and conditions that apply through this Agreement to Agency with respect to such information.

G. Individual Access. The Agency shall provide access, at the request of the County, to an Individual in order to meet the requirements under 45 CFR § 164.524.

H. Amendments to Protected Health Information. The Agency agrees to make any amendments to PHI that the County directs or agrees to pursuant to 45 CFR § 164.526 within ten (10) business days of the County's request.

I. Agency Compliance Records. The Agency shall make its internal practices, books and records, including policies and procedures relating to the use and disclosure of PHI received from, or created or received by Agency on behalf of the County available to the County in the time and manner designated by the County, for purposes of the County determining the Agency's compliance with the HIPAA privacy regulations.

J. Documentation and Accounting of Disclosures. The Agency shall document disclosures of PHI and information related to such disclosures as would be required for the County to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. The Agency further agrees to provide the County with such accounting within ten (10) business days of its request to respond to a request by an Individual for an accounting of disclosures in accordance with 45 CFR § 164.528.

IV. PERMITTED USE AND DISCLOSURE BY AGENCY

A. General Use and Disclosure. Except as otherwise limited by this Agreement or any Contract, the Agency may use or disclose PHI to perform its obligations and services to the County, provided that such use or disclosure would not violate the HIPAA privacy regulations if done by the County.

B. Specific Use and Disclosure Provisions.

1. Except as otherwise limited in this Agreement, the Agency may use PHI for the proper management and administration of any Contract or to carry out the legal responsibilities of the Agency.

2. Except as otherwise limited in this Agreement, the Agency may disclose PHI:

a. For the proper management and administration of the Agency, provided that disclosures are required by law; or

b. Agency obtains reasonable assurances from the person to whom the information is disclosed that it will:

i. Remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

ii. The person notifies the Agency of any instances of which it is aware in which the confidentiality of the information has been breached.

3. Except as otherwise limited in this Agreement, the Agency may use PHI to provide data aggregation services to the County as permitted by 42 CFR § 164.504(e)(2)(i)(B), if applicable.

4. The Agency may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 CFR § 164.502(j)(1).

V. OBLIGATION OF COUNTY

The County shall notify the Agency of any known future restrictions or limitations on the use of PHI that would affect Agency's performance of services under the Agreement, and Agency shall thereafter restrict or limit its uses and disclosures accordingly.

VI. TERMINATION FOR CAUSE

A. In addition to and notwithstanding the termination provisions in any Contract, upon the County's discovery of a material breach by Agency of the provisions of this Agreement, the County may:

1. Provide an opportunity for Agency to cure the breach or end the violation and terminate the Contract if Agency does not cure the breach or end the violation within the time specified by the County; or

2. Immediately terminate the Contract if Agency has breached a material term of the Contract and cure is not possible.

B. If neither termination nor cure is feasible, the County shall report the violation to the Secretary of the United States Department of Health and Human Services.

VII. DISPOSITION OF PROTECTED HEALTH INFORMATION UPON TERMINATION OR EXPIRATION

A. Except as provided in Section VII.B below, upon termination for any reason or expiration of the Contract, the Agency shall within ten (10) business days of such termination or expiration return or destroy all PHI received from the County, or created or received by the Agency on behalf of the County. This provision shall apply to PHI that is in the possession of subagencies or agents of Agency. The Agency shall retain no copies of the PHI.

B. In the event that the Agency determines that returning or destroying the PHI is infeasible, the Agency shall provide to the County notification of the conditions that make return or destruction infeasible. If return or destruction is infeasible, the Agency shall extend the protections of this Agreement to such PHI and limit further Uses and Disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as the Agency maintains such PHI. This provision shall survive termination of any Contract.

VIII. HITECH COMPLIANCE

A. The Agency acknowledges and agrees to follow the provisions of the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). The HITECH Act outlines the Agency's obligations when addressing privacy, security and breach of notification.

B. In the event of a breach of unsecured PHI or disclosure that compromises the privacy or integrity of PHI, the Agency shall take all measures required by state or federal law. The Agency shall provide the County with a copy of its investigative results and other information requested. The Agency shall report all PHI breaches to the County.

C. The Agency shall notify the County within one (1) business day by telephone and in writing of any acquisition, access, use or disclosure of PHI not allowed by the provisions of this Agreement of which it becomes aware, and of any instance where the PHI is subpoenaed, copied or removed by anyone except an authorized representative as outlined in 45 CFR §§164.304, 164.314 (a)(2)(C), 164.504(e)(2)(ii)(C), and 164.400-.414.

D. The Agency shall notify the County within one (1) business day by telephone or email of any potential breach of security or privacy. The Agency shall follow telephone or email notification with a secured faxed or other written explanation of the breach, to include the following: date and time of the breach; medium that contained the PHI; origination and destination of PHI; the Agency's personnel associated with the breach; detailed description of PHI; anticipated mitigation steps; and the name, address, telephone number, fax number, and email of the individual who is responsible for the mitigation. The Agency shall address communications to:

Snohomish County Human Services
3000 Rockefeller Avenue, MS 305
Everett, WA 98201.

IX. MISCELLANEOUS

A. No Third Party Beneficiaries. Nothing in this Agreement shall confer upon any person other than the parties and their respective successors or assigns any rights, remedies, obligations or liability whatsoever.

B. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the County to comply with the HIPAA and HITECH privacy regulations.

C. Amendments. The parties agree to take such action as is necessary to amend the requirements under this Agreement from time to time as is necessary for the County to comply with the requirements of the HIPAA and HITECH privacy regulations as may be amended or clarified by any applicable decision, interpretive policy or opinion of a court of the United States or governmental agency charged with the enforcement of the HIPAA and HITECH privacy regulations.

X. DATA SECURITY REQUIREMENTS

A. Data Transport.

When transporting Confidential Information electronically, including via email, the data will be protected by:

1. Transporting the data within the County network or Agency's internal network; or

2. Encrypting any data that will be in transit outside the County's network or Agency's internal network. This includes transit over the public Internet.

B. Protection of Data.

The Agency agrees to store data on one (1) or more of the following media and protect the data as described:

1. **Hard disk drives.** Data stored on local workstation hard disks. Access to the data will be restricted to authorized users by requiring logon to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms that provide equal or greater security, such as biometrics or smart cards.

2. **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 that 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 that 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.

3. For confidential data stored on these disks, deleting unneeded data is sufficient as long as the disks remain in a secured area and otherwise meets the requirements listed in the above paragraph. Destruction of the data as outlined in Section D. Data Disposition may be deferred until the disks are retired, replaced or otherwise taken out of the secure environment.

4. **Optical discs (CDs or DVDs) in local workstation optical disc drives.** Data provided by the County on optical discs that will be used in local workstation optical disc drives and that will not be transported out of a secure 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 that access said data on optical discs must be located in an area that is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

5. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers.** Data provided by the County on optical discs that will be attached to network servers and that 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 that 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.

6. **Paper documents.** Paper records must be protected by storing the records in a secure area that 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.

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

    a. County data shall not be stored by the Agency on portable devices or media unless specifically authorized within the Specific Terms and Conditions of the Contract. If so authorized, the data shall be given the following protections:

        1) Encrypt the data with a key length of at least 128 bits;

        2) Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics;

        3) 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;

        4) Physically protect the portable device(s) and/or media by:

            a) Keeping them in locked storage when not in use;

            b) Using check-in/check-out procedures when they are shared; and

            c) Taking frequent inventories.

    b. When being transported outside of a secure area, portable devices and media with confidential County data must be under the physical control of Agency staff with authorization to access the data.

    c. 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 secure area.

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

8. **Data Stored for Backup Purposes**

   a. Data may be stored on portable media as part of an Agency'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 Confidential Information still exists upon it, such media will be destroyed at that time in accordance with the disposition requirements in Section X.D Data Disposition.

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

C. Data Segregation.

1. County data must be segregated or otherwise distinguishable from non-County data. This is to ensure that when no longer needed by the Agency, all County data can be identified for return or destruction. It also aids in determining whether County data has or may have been compromised in the event of a security breach.

2. Electronic County data will be stored:

   a. On media (e.g., hard disk, optical disc, tape, etc.) which will contain no non-County data; or

   b. In a logical container on electronic media, such as a partition or folder dedicated to County data; or

   c. In a database which will contain no non-County data; or

   d. Within a database and will be distinguishable from non-County data by the value of a specific field or fields within database records;

3. When stored as physical paper documents, County data will be physically segregated from non-County data in a drawer, folder or other container.

4. When it is not feasible or practical to segregate County data from non- County data, then both the County data and the non-County data with which it is commingled must be protected as described in this Agreement.

D. Data Disposition.

When the contracted work has been completed or when no longer needed, except as noted in B.2 above, data shall be returned to the County or destroyed. Media on which data may be stored and associated acceptable methods of destruction are as follows:

Data stored on:	**Will be destroyed by:**
Server or workstation hard disks, or removable media (e.g., floppies, USB flash drives, portable hard disks, Zip or similar disks)	1. Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data; 2. Degaussing sufficiently to ensure that the data cannot be reconstructed; or 3. Physically destroying the disk.
Paper documents with sensitive or confidential data	Recycling through a contracted firm provided the contract with the recycler assures that the confidentiality of data will be protected.
Paper documents containing confidential information requiring special handling (e.g., PHI)	On-site shredding, pulping or incineration.
Optical discs (e.g., CDs or DVDs)	Incineration, shredding or completely defacing the readable surface with a course abrasive.
Magnetic tape	Degaussing, incinerating or crosscut shredding.

E. Notification of Compromise or Potential Compromise. The compromise or potential compromise of County shared data must be reported to the County contact designated in the Contract within one (1) business day of discovery.

E. Data shared with Subagencies. If County data provided under any Contract is to be shared with a subagency, the contract with the subagency must include all of the data security provisions within this Agreement and within any amendments, attachments or exhibits within any Contract. If the Agency cannot protect the data as articulated within this Agreement, then the contract with the subagency must be submitted to the County contact specified for the Contract for review and approval.

XI EFFECTIVE DATE

This Agreement becomes effective only upon incorporation by reference into a Contract between the County and the Agency.

FOR SNOHOMISH COUNTY:	FOR THE AGENCY:
Mary Jane Brell Vujovic, Director *(Date)* Department of Human Services	*(Signature)* *(Date)* *(Title)*

ATTACHMENT 1

Agency Agreement on Nondisclosure of Confidential Information

This form is for Agencies and other non-County employees.

CONFIDENTIAL INFORMATION
"Confidential Information" means information that is exempt from disclosure to the public or other unauthorized persons under Chapter 42.56 RCW or other federal or state laws. Confidential Information includes, but is not limited to, protected health information as defined by the federal rules adopted to implement the Health Insurance Portability and Accountability Act of 1996, 42 USC §1320d (HIPAA), and Personal Information. "Personal Information" means information identifiable to any person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, driver license numbers, other identifying numbers, and any financial identifiers.
REGULATORY REQUIREMENTS AND PENALTIES
State laws (including RCW 74.04.060 and RCW 70.02.020) and federal regulations (including HIPAA Privacy and Security Rules; 42 CFR, Part 2; 45 CFR Part 431) prohibit unauthorized access, use, or disclosure of Confidential Information. Violation of these laws may result in criminal or civil penalties or fines. You may face civil penalties for violating HIPAA Privacy and Security Rules up to $50,000 per violation and up to $1,500,000 per calendar year as well as criminal penalties up to $250,000 and ten years imprisonment.
ASSURANCE OF CONFIDENTIALITY
In consideration for Snohomish County granting me access to County property, systems, and Confidential Information, I agree that I: 1. Will not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Agreement for any purpose that is not directly connected with the performance of the contracted services except as allowed by law. 2. Will protect and maintain all Confidential Information gained by reason this Agreement against unauthorized use, access, disclosure, modification or loss. 3. Will employ reasonable security measures, including restricting access to Confidential Information by physically securing any computers, documents, or other media containing Confidential Information. 4. Have an authorized business requirement to access and use County systems or property, and view its data and Confidential Information if necessary. 5. Will access, use and/or disclose only the "minimum necessary" Confidential Information required to perform my assigned job duties. 6. Will not share County system passwords with anyone or allow others to use the County systems logged in as me. 7. Will not distribute, transfer or otherwise share any County software with anyone. 8. Understand the penalties and sanctions associated with unauthorized access or disclosure of Confidential Information. 9. Will forward all requests that I may receive to disclose Confidential Information to my supervisor for resolution. 10. Understand that my assurance of confidentiality and these requirements do not cease at the time I terminate my relationship with my employer or the County.
FREQUENCY OF EXECUTION AND DISPOSITION INSTRUCTIONS
This form will be read and signed by each non-County employee who has access to Confidential information and updated at least annually. Provide the non-County employee signor with a copy of this Assurance of Confidentiality and retain the original of each signed form on file for a minimum of six years.

SIGNATURE		
PRINT/TYPE NAME	NON-COUNTY EMPLOYEE'S SIGNATURE	DATE