ATTACHMENT 3

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 «VName»**,** 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. 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