

## ADMINISTRATIVE SERVICES AGREEMENT

This ADMINISTRATIVE SERVICES AGREEMENT (the "Agreement"), is effective the 1<sup>st</sup> day of January, 2020, (the "Effective Date") by and between Coordinated Care of Washington, Inc. ("CCW") and Salish Behavioral Health Administrative Services Organization, through Kitsap County, ("SBH-ASO"). Hereafter, CCW and SBH-ASO may be referred to individually as a "party" and collectively as the "parties."

### RECITALS

- A. **WHEREAS**, CCW is a Managed Care Organization and a licensed health care services contractor and provider of covered healthcare services to individuals enrolled in its benefit plans ("Members"), certified by the National Committee for Quality Assurance ("NCQA");
- B. **WHEREAS**, SBH-ASO is the Behavioral Health Administrative Services Organization ("BH-ASO"), contracted with the Washington State Health Care Authority ("HCA") and operating in the Salish Region;
- C. **WHEREAS**, the parties have agreed that SBH-ASO will provide the services contemplated by this Agreement, including the delegated functions described in Exhibit A, the Delegation Agreement, under the terms and conditions set forth herein;

**NOW THEREFORE**, in consideration of the commitments set forth below, the parties agree as follows:

- 1. **DEFINITIONS**. Capitalized terms not otherwise defined herein have the meanings given under the applicable HCA Contract(s).
  - 1.1 **CCW Policies**. "CCW Policies" means CCW-maintained policies and procedures, provided or made available to SBH-ASO.
  - 1.2 **CMS**. "CMS" means the Centers for Medicare and Medicaid Services, the federal agency within the United States Department of Health and Human Services that is responsible for the Medicare and Medicaid programs.
  - 1.3 **Compliance Requirements**. "Compliance Requirements" means: (i) state and federal law and regulation, applicable to CCW or to SBH-ASO; (ii) all HCA Contract requirements; (iii) applicable NCQA Standards; and (iv) the terms of this Agreement.
  - 1.4 **Delegated Function**. "Delegated Function" means a core business function that CCW is required to perform, and which a subcontractor is authorized to perform on CCW's behalf pursuant to a written agreement that requires ongoing oversight to ensure compliance with applicable Compliance Requirements.

**1.5 HCA Contracts.** "HCA Contracts" means CCW's contracts with the Washington State Health Care Authority for the Apple Health program, including the *Apple Health (Medicaid) managed care contract*, the *Apple Health – Fully Integrated Managed Care contract*, and the *Apple Health – Fully Integrated Managed Care – Behavioral Health Services wrap-around contract*.

**1.6 Project Data.** "Project Data" means: (i) all information processed or stored on computers or other electronic media by SBH-ASO on CCW's behalf; (ii) information that is provided by CCW or its affiliates to SBH-ASO to access, use, store, maintain, or transmit; and (iii) any information derived from such information. Project Data includes, without limitation: (i) information on paper or other non-electronic media provided to SBH-ASO for computer processing or storage, or information formerly on electronic media; (ii) information provided to SBH-ASO by CCW or information related to the Services performed under the Agreement that is provided to SBH-ASO by a third party; and (iii) any Patient Identifying Information, as that term is defined in 42 C.F.R. §2.11, or Protected Health Information, as that term is defined in 45 C.F.R. §160.103 ("PHI"), that SBH-ASO receives from or on behalf of CCW

**1.7 Subdelegate.** "Subdelegate" means a subcontractor of SBH-ASO who CCW has approved in writing to perform all or part of a Delegated Function under this Agreement. -

**1.8 Health Care Authority.** "Health Care Authority" or "HCA" shall mean the Washington State Health Care Authority, the single-state agency responsible for Washington State's Medicaid programs, referred to as "Apple Health".

## **2. SERVICES**

**2.1** As used herein, "Services" includes SBH-ASO's performance of all contracted services, including any Delegated Functions.

**2.2 Compliance.** SBH-ASO shall perform the Services in accordance with applicable Compliance Requirements. To the extent that a Compliance Requirement related to this Agreement is not directly applicable to SBH-ASO, SBH-ASO shall perform its obligations in a manner that enables CCW to comply with such Compliance Requirement.

**2.2.1** The Services will be performed in a professional, competent, and timely manner by appropriately qualified personnel that have the requisite knowledge, training, ability, and licensure or credentials to perform the Services in accordance with applicable Compliance Requirements and industry standards.

**2.2.2** SBH-ASO shall comply with the Program Integrity requirements contained in the HCA Contracts, including the requirement to immediately report to CCW any instance of actual or potential Fraud of which SBH-ASO becomes aware, and CCW's HCA-approved Program Integrity Policies.

2.2.3 The parties acknowledge that Compliance Requirements may be amended during the term of this Agreement. Each party shall modify its performance to ensure ongoing compliance with applicable Compliance Requirements, as amended.

### **3. SBH-ASO OBLIGATIONS**

3.1 SBH-ASO shall cooperate with and participate in CCW's monitoring and oversight activities, which shall be performed in accordance with applicable Compliance Requirements CCW Policies, and industry standards.

3.2 Upon CCW's request, SBH-ASO shall provide to CCW any information necessary for CCW to meet its obligations under the HCA Contracts.

3.3 **Required Disclosures**. In accordance with HCA and CMS requirements, SBH-ASO is required to make certain disclosures to CCW concerning SBH-ASO's ownership and control, information on persons convicted of crimes, and other sensitive matters. SBH-ASO shall comply with all disclosure requirements as set forth herein, or as required by applicable Compliance Requirements.

3.3.1 SBH-ASO shall complete CCW's "Ownership and Control Interest Disclosure Form" ("OCID Form") upon execution of this Agreement, upon CCW's request, and within 35 business days of any change in the information provided by SBH-ASO on the OCID Form. This Agreement shall not be deemed effective unless and until SBH-ASO executes and returns to CCW a completed OCID Form.

3.3.2 **Additional Disclosure Requirements**. Within 35 calendar days of CCW's request, SBH-ASO shall provide to CCW:

3.3.2.1 Full and complete business information concerning: (i) the ownership of any subcontractor with whom SBH-ASO has had more than \$25,000.00 of business transactions within the 12-month period prior to the date of the request; and (ii) any significant business transactions between SBH-ASO and any wholly owned supplier, or between SBH-ASO and any of its subcontractors, during the 5-year period prior to the date of the request.

3.3.2.2 A description of any transactions between SBH-ASO and a "party in interest," as defined in Section 1318(b) of the Public Health Service Act, including: (i) the sale, lease or exchange of any property; (ii) the furnishing for consideration of goods, services (including management services), or facilities, but not including salaries paid to employees for services provided in the normal course of their employment; and (iii) the lending of money or other extension of credit.

3.3.3 **Information on Persons Convicted of Crimes**. Upon execution of this Agreement and upon CCW's request thereafter, SBH-ASO shall investigate and disclose to CCW the identity of any individual who has been convicted of a criminal offense related to that person's participation in a federally funded health care program,

including Medicaid, Medicare, and the Children's Health Insurance Program, since the inception of those programs, and who is: (i) a person who has an ownership or control interest in SBH-ASO; (ii) an agent or person who has been delegated the authority to obligate or act on behalf of SBH-ASO; or (iii) an agent, managing employee, general manager, business manager, administrative, director, or other individual who exercises operational or managerial control over, or who directly or indirectly conducts, SBH-ASO's day-to-day operations.

**3.4 Licenses and Registrations.** SBH-ASO has and will maintain the licenses, permits, registrations, certifications, and other governmental authorizations necessary to conduct its business or perform the Services. SBH-ASO shall notify CCW in the event of a change in status of any required license, permit, registration, certification, or other authorization necessary for SBH-ASO's performance under this Agreement.

**3.5 No Exclusion.** SBH-ASO represents and warrants that itself and its employees, directors, officers, and agents are not now and never have been: (i) sanctioned under a federal or state program or law; (ii) listed in the current List of Excluded Individuals and Entities by the Office of the Inspector General for the U.S. Department of Health and Human Services; (iii) listed on the General Services Administration's List of Parties Excluded from Federal Programs; (iv) otherwise excluded from participation in any federally-funded health care program, including Medicare and Medicaid.; or (v) convicted of a serious crime directly related to healthcare. SBH-ASO shall immediately notify CCW of any threatened, proposed, or actual change in the foregoing representations.

**3.6 Subcontractors.** If SBH-ASO subcontracts any part of its performance hereunder, it must enter a written agreement with the subcontractor, which must require the subcontractor to comply with applicable Compliance Requirements and CCW Policies. Any such subcontract shall also require the subcontractor to perform in a manner that enables CCW to comply with such Compliance Requirements and CCW Policies, regardless of whether such requirements are directly applicable to SBH-ASO or subcontractor.

3.6.1 SBH-ASO shall screen all new and existing subcontractors against the lists of excluded individuals referenced in Section 3.5, as well as applicable state-maintained exclusion list(s). If a SBH-ASO subcontractor is determined to be debarred, suspended, or otherwise excluded from receiving a subcontract funded in whole or in part by federal or state dollars, including Medicaid funds, SBH-ASO will immediately terminate its relationship with such subcontractor.

3.6.2 SBH-ASO may not subcontract any part of its performance of a Delegated Function without the prior written approval of CCW. If CCW approves a SBH-ASO Subdelegate to perform all or part of a Delegated Function hereunder, SBH-ASO shall ensure compliance with Exhibit A for itself and its Subdelegate.

**Taxes.** SBH-ASO will pay all taxes on its income as well as all compensation, taxes, and insurance associated with its employees. Neither SBH-ASO nor its representatives, employees, agents, or subcontractors, shall have any claim against CCW for vacation pay,

sick leave, retirement benefits, social security, worker's compensation, health or disability benefits, unemployment insurance benefits, or employee benefits of any kind arising from SBH-ASO's performance under this Agreement.

**3.7 Insurance.** At its sole expense and through the term of this Agreement, SBH-ASO shall maintain the following insurance and coverage amounts to cover its provision of Services hereunder: (i) One Million Dollars (\$1,000,000) per occurrence and Two Million Dollars (\$2,000,000) annual aggregate for commercial general liability; (ii) applicable state statutory limits for workers' compensation; and (iii) any other usual and customary policies of insurance applicable to SBH-ASO or the Services being performed.

3.7.1 By requiring insurance, CCW does not represent that such coverage or limits will be adequate to protect SBH-ASO. Such coverage and limits shall not be deemed as a limitation on SBH-ASO's liability under the indemnities granted herein.

3.7.2 SBH-ASO will obtain all insurance coverage specified herein from insurers with a current A.M. Best financial rating of A-, Class VII or better. All policies shall be primary with respect to any insurance maintained by SBH-ASO.

3.7.3 If SBH-ASO procures a "claims-made" policy to meet the insurance requirements herein, SBH-ASO shall purchase "tail" coverage that provides for an indefinite reporting period upon the termination of any such policy or upon termination of this Agreement.

3.7.4 SBH-ASO will promptly notify CCW of any material change in the carrier or in the amount or scope of required coverage. SBH-ASO shall provide a certificate of insurance coverage within ten (10) days of CCW's request. SBH-ASO's failure to maintain required insurance constitutes a material breach of this Agreement.

#### **4. MCO OBLIGATIONS**

4.1. **Taxes.** CCW will pay applicable federal, state, and local taxes including sales, use, service, or other such taxes associated with its receipt of the Services.

4.2. **CCW Premises.** If SBH-ASO provides Services on CCW premises, CCW will provide SBH-ASO the space, furniture, fixtures, equipment, and supplies that CCW, in its sole discretion, deems reasonably necessary for the provision of Services. SBH-ASO shall use any space, furniture, fixtures, equipment, or supplies provided by CCW only for the performance of the Services covered by this Agreement, and not for any other purpose, including SBH-ASO's own private use. If SBH-ASO provides Services on CCW premises, SBH-ASO's on-site personnel will be required to follow applicable CCW protocols and complete any required training for on-site personnel.

4.3. **Legal Responsibility.** Nothing in this Agreement terminates or modifies CCW's legal responsibility to carry out its obligations under the HCA Contracts. CCW shall remain responsible for oversight of all functions and responsibilities subcontracted to SBH-ASO.

4.4. **Oversight and Ongoing Monitoring.** CCW will monitor SBH-ASO's performance hereunder on an ongoing basis and subject SBH-ASO to formal review, consistent with Compliance Requirements, CCW Policies, and industry standards. Formal review will be completed at least once every three (3) years. Such review shall be based on the specific activities contracted hereunder, and shall address compliance with applicable Compliance Requirements.

4.5. **CCW's Grievance and Appeals System.** CCW has provided SBH-ASO information regarding CCW's grievance system, including: (i) the toll-free numbers to file oral grievances and appeals; (ii) the availability of assistance in filing; (iii) a Member's right to request continuation of benefits during an appeal or hearing and, if CCW's action is upheld, the Member's responsibility to pay for the continued benefits; (iv) a Member's right to file grievances and appeals, the ability of their provider to file a grievance or appeal on the Member's behalf, and the requirements and timeframes for filing; and (v) a Member's right to a hearing, how to obtain a hearing, and representation rules at a hearing. Information regarding CCW's grievance system is available online at <https://www.coordinatedcarehealth.com/members/medicaid/resources/complaints-appeals.html>

## **5. COMPENSATION AND PAYMENT**

5.1 All fees, reimbursement, payment, and other compensation related to SBH-ASO's performance hereunder are set forth in ATTACHMENT C.

5.2 SBH-ASO shall accept as payment in full the compensation set forth in ATTACHMENT C, and shall make no request for payment from HCA or any Member for services rendered under this Agreement. SBH-ASO, for itself and its representatives, employees, agents, and subcontractors, shall hold HCA, HCA employees, and all Members, harmless in the event of non-payment by CCW under the Agreement.

5.3 **Overpayment or Underpayment.** SBH-ASO shall reimburse CCW for any overpayment made hereunder within thirty (30) days of SBH-ASO's discovery or CCW's written notification of such overpayment. CCW shall remit to SBH-ASO any underpayment within thirty (30) days of receipt of SBH-ASO's invoice substantiating such underpayment. Upon reasonable notice of intent, each party has the right of offset as to any amounts owed to either party against any amount owed by the other party.

5.4 **Federal Funds.** Each party is subject to the laws applicable to individuals and entities receiving federal funds, and shall inform all related entities and subcontractors that payments they receive are, in whole or in part, from federal funds. This Agreement shall be interpreted and performed in a manner that results in compliance with such laws.

## **6. TERM and TERMINATION**

6.1. **Term.** This Agreement shall be effective upon the Effective Date and shall terminate on December 31, 2020 (“Term”), unless extended by mutual written agreement of the parties, or terminated as provided herein.

6.2. **Termination.** This Agreement may be terminated prior to the expiration of the Term as follows:

6.2.1. **Termination For Cause.** Either party may terminate this Agreement for cause upon ninety (90) days’ prior written notice to the other party specifying the cause for termination. The alleged violating party shall have ninety (90) days to rectify the specified cause, and if the cause is not rectified within that ninety (90) day period, the terminating party may terminate this Agreement upon written notice to the other party. “Cause” for termination includes a party’s material breach of its obligations under this Agreement.

6.2.2. **Exclusion.** If either party is excluded from participation in Medicare or Medicaid or if for any reason a party’s performance under this Agreement is deemed illegal or unethical by a recognized body in the insurance or healthcare industry, then this Agreement shall automatically terminate.

6.2.3. **Termination of HCA Contract(s) or Service Area(s).** In the event that one or more HCA Contracts expires or is terminated, or CCW is no longer contracted as a Medicaid Managed Care Organization in an applicable service area, CCW may terminate the Agreement upon written notice to SBH-ASO.

6.2.4. **Termination of BH-ASO Contract.** In the event that SBH-ASO’s BH-ASO contract with HCA expires or is terminated prior to the end of the Term of this Agreement, this Agreement shall immediately terminate.

6.2.5. **Bankruptcy.** If an assignment of a party’s business for the benefit of creditors is made, if a petition in bankruptcy is filed by or against a party, if a receiver or similar officer is appointed to take charge of all or part of a party’s property, or if a party is adjudicated bankrupt, the other party may terminate this Agreement upon written notice to the other party.

6.2.6. **Failure to Meet Pre-Conditions of Delegation.** If SBH-ASO’s performance under this Agreement contemplates performance of any part of a Delegated Function, and SBH-ASO fails to meet CCW’s pre-delegation requirements, CCW may terminate this Agreement upon written notice to SBH-ASO.

6.3. **Effect of Termination or Expiration.**

6.3.1. **Termination or Suspension of Delegated Function.** Termination or suspension of SBH-ASO’s performance of a Delegated Function, in whole or in part, shall not terminate or suspend this Agreement.

- 6.3.2. **Existing Obligations Not Released.** Rights, liabilities, and other obligations of the parties arising or incurred prior to the date of termination or expiration of this Agreement are not terminated by the termination or expiration hereof.
- 6.3.3. **Ongoing Cooperation.** The parties shall cooperate to ensure an efficient transition of the Services. SBH-ASO shall provide to CCW all Program Data, and any other documentation or information necessary to transition the Services to CCW or its third party designee. If requested by a party, SBH-ASO and CCW will develop a mutually agreed upon transition plan to ensure the orderly transition of the Services and each party's ongoing compliance with applicable Compliance Requirements.
- 6.3.4. **Financial Reconciliation.** The parties shall reconcile and true up their financial relationship upon termination or expiration of this Agreement.
- 6.3.5. **Survival.** All terms and conditions of this Agreement, which expressly or by their nature should survive termination or expiration hereof, shall survive termination or expiration of this Agreement.

## **7. CONFIDENTIALITY**

7.1. This Agreement, including all exhibits, attachments and other addenda hereto, contains the Work Product and other confidential and/or proprietary information of the parties. Neither party will disclose any term or condition hereof to a third party, except: as expressly permitted herein; to ensure a Party's compliance with applicable Compliance Requirements; or with the express, written permission of the other party.

7.2. **Confidential Information.** Each party shall keep confidential the other party's proprietary or confidential information, including the terms and conditions of this Agreement, and all information related to finances, methods of operation and competition, pricing, operations, personnel, Members, patients, computer programs and files, business strategies including cost data, utilization review techniques, medical management, quality assurance protocols, patents, trade secrets, know-how and other proprietary processes, and information included in manuals or memoranda, as they may now exist or may be developed or amended, including all Project Data and any Work Product or other information that SBH-ASO generates in its performance hereunder (collectively, "Confidential Information").

7.3. **No Disclosure of Confidential Information.** Neither party shall disclose the other party's Confidential Information, in whole or in part, directly or indirectly, to any person, firm, association or other entity for any unauthorized purpose, nor shall a party use any Confidential Information for its own purposes or for the benefit of any other person, firm, or entity unless: (i) such information is or becomes generally available to the public other than as a result of an unauthorized disclosure by the disclosing party; (ii) such information is required to be disclosed by law or by a judicial, administrative, or regulatory authority; or (iii) as necessary to enforce its rights and perform its agreements and obligations hereunder. Neither party shall reverse engineer, disassemble, or decompile any prototypes, software or other tangible objects which embody the other party's Confidential Information. Neither party shall use the other's name, logo, trademark,



or other identifying information or make any public communication or advertisement without the express written consent of the other party.

## **8. DATA SHARING; DATA SECURITY.**

### **8.1. Additional Definitions.**

8.1.1. **Data Breach.** “Data Breach” means unauthorized disclosure or exposure of Project Data.

8.1.2. **HIPAA.** “HIPAA” shall mean the Health Insurance Portability and Accountability Act of 1996.

8.1.3. **HIPAA Rules.** “HIPAA Rules” shall mean the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule.

### **8.2. Data Management.**

8.2.1. SBH-ASO shall not access, use, or disclose Project Data in any manner that would constitute a violation of state or federal law or regulation, or this Agreement.

8.2.2. SBH-ASO shall not outsource, share, or retransfer Project Data to any person or entity, except to employees, agents, or subcontractors of SBH-ASO who must access or use Project Data in the performance of SBH-ASO’s duties under this Agreement.

8.2.3. SBH-ASO will not permit any third party to access Project Data unless such third party is subject to a written agreement with SBH-ASO that incorporates the Data Management and Data Security requirements of this Article 8 of the Agreement. SBH-ASO will ensure that each such third party complies with all of the terms of this Agreement related to Project Data.

8.2.4. SBH-ASO will not access, use, process, or disclose Project Data other than as necessary to perform its obligations under this Agreement. Notwithstanding the foregoing, SBH-ASO may disclose Project Data as required by law. In such cases, SBH-ASO shall provide CCW with prompt written notice of any such legal or governmental demand and shall cooperate with CCW in any effort to seek a protective order or otherwise contest such required disclosure.

8.2.5. CCW possesses and retains all rights, title, and interest in and to Project Data, and SBH-ASO’s use and possession of Project Data is solely on CCW’s behalf and for the benefit of CCW. CCW may access and copy any Project Data in SBH-ASO’s or a third party’s possession at any time, and SBH-ASO will reasonably facilitate such access and copying promptly after CCW’s request.

8.2.6. In its handling of Project Data, SBH-ASO will comply with applicable Compliance Requirements and CCW Policies.

**8.2.7. Unless prohibited by Article 10 or SBH-ASO's independent legal obligations, upon expiration or termination of this Agreement, SBH-ASO will return to CCW or destroy all Project Data in whatever form or medium, including all copies thereof and all data, compilations, and other works derived therefrom. This provision shall apply to any Project Data that is in SBH-ASO's possession or the possession of any individual or entity that received Project Data from SBH-ASO.**

**8.2.7.1. SBH-ASO will identify, in the form and manner requested by CCW, any Project Data, including any Project Data that SBH-ASO has disclosed to third parties, that cannot feasibly be returned to CCW or destroyed, and explain why return or destruction is infeasible. SBH-ASO will limit its further use or disclosure of such Project Data to those purposes that make return or destruction infeasible. SBH-ASO will, by its written agreement with any third party, require such third party to limit its further use or disclosure of the Project Data that the third party cannot feasibly return or destroy to those purposes that make the return or destruction of such information infeasible. SBH-ASO will complete these obligations as promptly as possible, but not later than thirty (30) calendar days following the effective date of termination or expiration of this Agreement.**

**8.2.7.2. SBH-ASO shall require any such third party to certify to SBH-ASO that it has returned or destroyed all Project Data that could be returned or destroyed. SBH-ASO will require any such third party to complete these obligations as promptly as possible, but not later than thirty (30) calendar days following the effective date of termination or expiration of this Agreement.**

**8.2.7.3. SBH-ASO's obligations to protect the privacy and safeguard the security of Project Data as specified in this Agreement will be continuous and will survive the termination or conclusion of this Agreement.**

**8.3. Data Security. In addition to the requirements of this Article 8, SBH-ASO will, at all times, exercise reasonable efforts to prevent the unauthorized access, use, or disclosure of Project Data.**

**8.3.1. SBH-ASO will maintain, implement, and comply with a written data security program that requires commercially reasonable policies and procedures to ensure compliance with the Data Security requirements of this Agreement as well as applicable Compliance Requirements.**

**8.3.1.1. SBH-ASO's data security policies and procedures will contain administrative, technical, and physical safeguards, including without limitation:**

**8.3.1.1.1. Guidelines on the proper disposal of Project Data after it is no longer needed to carry out the purposes of the Agreement;**

- 8.3.1.1.2. Access controls on electronic systems used to store, maintain, access, or transmit Project Data;
- 8.3.1.1.3. Access restrictions at physical locations containing Project Data;
- 8.3.1.1.4. Encryption of electronic Project Data;
- 8.3.1.1.5. Two-factor authentication procedures;
- 8.3.1.1.6. Testing and monitoring of electronic systems; and
- 8.3.1.1.7. Procedures to detect actual and attempted attacks on or intrusions into the systems containing or accessing Project Data.

8.3.1.2. SBH-ASO will review its data security policies and procedures and all other Project Data security precautions regularly, but no less frequently than annually, and will update and maintain policies, procedures, and practices to comply with applicable Compliance Requirements, changes in technology, and industry best practices.

8.3.1.3. SBH-ASO's written data security program shall meet or exceed the requirements of the HIPAA Rules, as currently in effect or later amended.

8.3.2. SBH-ASO will implement and maintain a program for managing actual or suspected Data Breaches.

8.3.2.1. SBH-ASO will report to CCW's Compliance Officer any actual or potential Data Breach immediately and not more than seventy-two (72) hours after SBH-ASO discovers such actual or potential Data Breach. SBH-ASO's report will include at least the following, provided that the absence of any information will not be cause for SBH-ASO to delay the report, and additional information will be provided in a subsequent report as soon as reasonably possible:

- 8.3.2.1.1. Identify the nature of the Data Breach, including a brief description of what happened, the date of the Data Breach and the date of the discovery of the Data Breach, and the number of individuals whose information may have been the subject of the Data Breach;
- 8.3.2.1.2. Identify the types of information that were involved in the Data Breach, and to the extent the Data Breach involved PHI, identify the types of PHI;
- 8.3.2.1.3. Identify who made the non-permitted use or disclosure and who received the non-permitted disclosure;

8.3.2.1.4. Identify what corrective of investigational action SBH-ASO took or will take to prevent further non-permitted uses or disclosures, to mitigate harmful effects, and to protect against any further Data Breaches;

8.3.2.1.5. Identify what steps the individuals who were the subjects of or affected by the Data Breach should take to protect themselves; and

8.3.2.1.6. Provide such other information as CCW may request.

8.3.2.2. In the event of a Data Breach, SBH-ASO shall immediately take such actions as may be necessary to preserve forensic evidence and eliminate the cause of the Data Breach.

8.3.2.3. SBH-ASO shall cooperate with CCW and law enforcement agencies, where applicable, to investigate and resolve the Data Breach, including without limitation by providing reasonable assistance to CCW in notifying affected individuals and/or entities. SBH-ASO will give CCW prompt access to such records related to a Data Breach as CCW may reasonably request; provided such records will be SBH-ASO's Confidential Information and SBH-ASO will not be required to provide CCW with records belonging to its other customers. The provisions of this subsection do not limit CCW's other rights or remedies, if any, resulting from a Data Breach.

8.3.2.4. SBH-ASO shall defend, indemnify, and hold CCW harmless from and against any claims, actions, loss, liability, damage, costs, or expenses, including but not limited to reasonable attorneys' fees, arising from any or all Data Breaches. The indemnification provided hereunder includes the full costs of forensic analysis, system remediation to eliminate the cause of the Data Breach, and notice to affected individuals, including but not limited to the services of a third party firm.

8.4. **Disaster Plan** SBH-ASO will maintain a Disaster Recovery and Business Continuation Plan ("Disaster Plan") that sets forth a strategy to reasonably respond to an event that impacts SBH-ASO's ability to timely perform its obligations under this Agreement, including a system breakdown and natural or man-made disasters. The Disaster Plan will include application and system recovery and/or manual procedures as well as operating procedures to enable continued provision of Services within forty-eight (48) hours of a disaster or system failure.

8.4.1. SBH-ASO will maintain or contract for a computing environment which includes the required hardware, software, network, power, and other related equipment or supplies necessary to execute the Disaster Plan.

8.4.2. SBH-ASO will test its Disaster Plan in accordance with the requirements of the HIPAA Security Rule, and at least annually and in the event of a material change in

the computing environment. SBH-ASO will provide CCW with the results of such tests.

8.4.3. CCW or its designee may audit SBH-ASO's Disaster Plan to monitor compliance with this Section 8.4.

8.5. **Business Associate Agreement.** Under this Agreement, SBH-ASO is a Business Associate, as that term is defined in 45 C.F.R. §160.103, of CCW. As such, the parties have entered a Business Associate Agreement, which is attached hereto and by this reference incorporated herein as Exhibit [X]. In the event of a conflict between the terms of the Business Associate Agreement and these Data Security requirements, the terms of the Business Associate Agreement shall prevail in all cases involving PHI. Notwithstanding the foregoing, SBH-ASO shall be obligated to comply with the Data Security requirements so long as such compliance does not violate the terms of the Business Associate Agreement.

8.6. **Alcohol and Substance Abuse Records.** Each party acknowledges and agrees that if it receives, stores, processes, has access to, maintains, or otherwise deals with Patient Identifying Information from an alcohol or drug abuse "program", as defined in 42 C.F.R. §2.11, that is federally assisted in the manner described in 42 C.F.R. §2.12(b), then it is fully bound by the federal regulations governing Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. Part 2, with respect to such information and records, including but not limited to the duty to resist in judicial proceedings any efforts to obtain access to such information or records, other than as permitted by law.

## 9. **INDEMNIFICATION**

9.1. **CCW Indemnity.** CCW, for itself, its legal representatives, and its lawful successors and assigns, shall indemnify, defend, and hold harmless SBH-ASO, and its officers, employees, and agents, from any claim, liability, loss, demand, cost, and expense of any kind, including reasonable attorney's fees and any disbursements, or regulatory penalties (collectively, the "Loss") that the SBH-ASO may hereafter incur, sustain, or be required to pay by reason of CCW's breach of the Agreement or from the reckless, negligent, or intentional acts or omissions of CCW or its officers, employees, subcontractors, or agents.

9.2. **SBH-ASO Indemnity.** SBH-ASO, for itself, its legal representatives, and its lawful successors and assigns, shall indemnify, defend, and hold harmless CCW, and its officers, employees, and agents, from any claim, liability, demand, cost and expense of any kind, including reasonable attorney's fees and disbursements, or regulatory penalties (collectively, the "Loss") that CCW may hereafter incur, sustain, or be required to pay by reason of SBH-ASO's breach of the Agreement, or from the reckless, negligent, or intentional acts or omissions of SBH-ASO or its officers, employees, subcontractors, or agents. SBH-ASO shall further indemnify and hold harmless HCA and HCA employees against all injuries, deaths, losses, damages, claims, suits, liabilities, judgments, costs and expenses which may in any manner accrue against HCA or its employees through the intentional misconduct, negligence, or omission of SBH-ASO or its officers, employees, subcontractors, or agents.

9.3. **Notice and Process.** Once the party entitled to indemnification under this Article 9 receives notice of a Loss for which such party will seek indemnification from the other party, the indemnified party will promptly notify the other party in writing. Such notice will describe any matters related to or with respect to the Loss of which the indemnified party has knowledge. However, failure to notify the indemnifying party of such a Loss will not relieve the indemnifying party of its obligations under this Article 9, except to the extent that the indemnifying party is prejudiced by such failure. The indemnified party will give the indemnifying party the opportunity to control the response to the Loss, and any defense thereof, including without limitation, any agreement related to the settlement thereof; provided, however, that the indemnified party may participate, at its own expense, in any defense and any settlement, directly or through counsel of its choice. As soon as reasonably practicable after receiving written notice of the Loss, the indemnifying party will notify the indemnified party in writing as to whether the indemnifying party elects to assume control of the response, or any defense or settlement related to such Loss. If the indemnifying party elects not to assume such control, the indemnified party will have the right to respond to, defend, or settle the Loss as it may deem appropriate, at the cost and expense of the indemnifying party, which will promptly reimburse the indemnified party for such costs, expenses, and settlement amounts.

9.4. **Subrogation.** If an indemnifying party is obligated to indemnify an indemnified party under this Article 9, then, upon paying that indemnity in full, the indemnifying party will be subrogated to all rights of the indemnified party concerning the Loss to which the indemnification relates.

## **10. MONITORING AND OVERSIGHT; RECORD RETENTION**

10.1. **Records.** Each party shall prepare, protect, and maintain appropriate records, including administrative, medical, and financial records, covering its performance under this Agreement, including the provision of Services, for at least ten (10) years from the later of (i) the date the Agreement terminates or expires, (ii) the date any inspection, audit, litigation or other action related to the records or their content concludes, or (iii) the date of final payment under the applicable HCA Contract(s). Financial records will follow generally accepted accounting principles. Upon reasonable notice, each party shall provide access to the other to inspect or audit its records related to this Agreement.

10.2. **Government Inspection and Auditing.** Each party shall permit, at any time, the State of Washington, including HCA, the Washington Medicaid Fraud Control Division ("MFCD"), and state auditor, the Secretary of the U.S. Department of Health and Human Services ("HHS"), the HHS Office of the Inspector General, CMS, the U.S. Government Accountability Office, the U.S. Office of Management and Budget, the Comptroller General, and their respective designees, to access, inspect and audit any records or documents of SBH-ASO or its subcontractors, and shall permit inspection of the premises, physical facilities, and equipment where Medicaid-related activities or work is conducted at any time.

10.2.1. Each party shall forthwith produce all documents, records and other data requested as part of such an inspection, audit, review, investigation or evaluation. If the requesting agency asks for copies of records, documents, or other data, each party

shall make copies of such records at no charge to the requestor and shall deliver them to the requestor within 30 calendar days of the request, or any shorter time as authorized by law or court order.

## **11. DISPUTE RESOLUTION**

11.1. **Informal Resolution.** Each party shall cooperate in good faith and deal fairly in its performance hereunder to accomplish the parties' objectives and avoid disputes. The parties will promptly meet and confer to resolve any disputes that may arise.

11.2. **Mediation.** If a dispute is not resolved through conference, the parties will participate and equally share in the expenses of a mediation conducted by a neutral third-party professional in Seattle, Washington.

11.3. **Arbitration.** If the dispute is not resolved through mediation, either party may request binding arbitration. If the other party agrees, such arbitration shall be conducted in Seattle, Washington in accordance with the American Health Lawyers Association Alternative Dispute Resolution Service Rules of Procedure for Arbitration. The final decision of the arbitrator shall be set forth in writing and signed by the arbitrator and be binding on each party. Nothing herein will prevent either party from seeking injunctive relief or provisional relief in an appropriate forum to protect or preserve such party's rights.

## **12. COMPLIANCE WITH LAWS**

12.1. **Compliance with Laws.** Each party will comply with applicable federal, state, and local laws and regulations, as amended, including but not limited to those specifically identified under the *Compliance with Applicable Law* Sections in the respective HCA Contracts.

12.2. **Non-Discrimination.** Neither party shall discriminate against any person because of race, color, national origin, ancestry, religion, gender, marital status, age, sexual orientation, health status, presence of a sensory, mental or physical disability, use of a service animal, or any other reason(s) prohibited by law. Neither party shall use any policy or procedure which has the effect of discriminating on the basis of any of the foregoing.

12.3. **Accommodations.** SBH-ASO shall make reasonable accommodations, as required by state and federal law, to ensure Members with disabilities are able to access and take full advantage of the Services on an equal basis with all other Members.

12.4. **Enrollee Rights.** SBH-ASO shall comply with any applicable federal and state laws that pertain to Member rights, and ensure that its staff and providers protect and promote those rights when furnishing Services to Members.

## **13. GENERAL**

13.1. **Independent Contractor.** CCW and SBH-ASO are separate legal entities and independent contracting parties. Each party shall exercise ultimate control over its assets, operations, employees, and subcontractors, and retain ultimate authority and responsibility in exercising its powers, duties, and responsibilities, subject to the rights and responsibilities assumed under this Agreement.

13.2. **Work Product.** CCW shall retain full ownership and title to, and all other rights in, any data, materials, forms, equipment, and supplies obtained by SBH-ASO from or on behalf of CCW, including Project Data and all CCW Confidential Information. Works of authorship, reports, deliverables, and inventions that are designed, created, developed, or conceived in connection with the Services (collectively, the "Work Product") will be considered "works made for hire" as defined in the Copyright Act at 17 U.S.C. § 101. To the extent the Work Product is not "works made for hire," SBH-ASO hereby assigns all rights in the Work Product to CCW. SBH-ASO will execute any assignments and any other documents, and take any other action CCW reasonably requests, without payment of additional consideration, as may be necessary or advisable to convey full ownership of all intellectual property rights to the Work Product and to protect CCW's interest in the Work Product. This ownership provision does not apply to SBH-ASO's pre-existing intellectual property or to any invention or other creative works for which no CCW data, equipment, supplies, facility, or Confidential Information was used, which was developed entirely on SBH-ASO's own time, and which do not relate to CCW activities or the Services.

13.3. **Use of a Party's Marks.** Neither party shall use the other's name, logo, trademark, or other identifying information, or make any public communication or advertisement related to this Agreement or a party's performance hereunder, without the express written consent of the other party.

13.4. **Notice.** All notices or other communications required or permitted to be given hereunder shall be in writing and deemed to have been delivered to a party upon: (i) personal delivery to that party; (ii) if simultaneously mailed as provided herein, upon electronically confirmed delivery by facsimile to the telephone number provided by the party for such purposes; (iii) upon deposit for overnight delivery with a bonded courier holding itself out to the public as providing such services, with charges prepaid; or (iv) four (4) business days following deposit with the United States Postal Service, postage prepaid, and in any case addressed to the party as set forth below, or to another address that the party provides by notice to the other party:



<p>Coordinated Care of Washington  Attn: President and CEO  1145 Broadway Suite 300  Tacoma, WA 98402</p> <p>With copy to Legal Department  Email: <a href="mailto:kathornton@centene.com">kathornton@centene.com</a>  <a href="mailto:rbush@centene.com">rbush@centene.com</a>  <a href="mailto:contracting@coordinatedcarehealth.com">contracting@coordinatedcarehealth.com</a></p>	<p>Salish Behavioral Health Administrative Services Organization:  Attn: <u>Regional Administrator</u>  <u>614 Division Street, MS-23</u>  <u>Port Orchard, WA 98366</u></p> <p>Email: <u>gilewis@co.kitsap.wa.us</u></p>
---	---

13.5. **Expenses.** Except as specifically provided herein, each party shall bear its own expenses related to its performance hereunder, including legal and accounting fees.

13.6. **Assignment.** SBH-ASO may not assign or transfer this Agreement without CCW's prior written consent. Any assignment without such consent shall be of no force and effect. CCW may not assign this Agreement without the prior written approval of the HCA. This Agreement shall be binding on the parties' successors and lawful assigns.

13.7. **State Subrogation.** In the event that any government entity undertakes a criminal, civil, or administrative action recovery against an entity that has directly or indirectly received funds under this Agreement, SBH-ASO agrees to subrogate to the State of Washington any claims arising under this Agreement that SBH-ASO has or may have against the entity from which recovery is sought.

13.8. **Choice of Law; Venue.** This Agreement shall be governed by and construed in accordance with the laws of the State of Washington, without reference to conflict of laws principles, except to the extent pre-empted by federal law. All disputes arising from or relating to this Agreement will be within the exclusive jurisdiction of the state and/or federal courts located in Seattle, Washington, and the parties hereby consent to such exclusive jurisdiction and waive any objections to venue.

13.9. **No Third Party Rights.** Nothing herein shall be construed or be deemed to create any rights or remedies in or for the benefit of any third party.

13.10. **Entire Agreement.** This Agreement, including all attachments, exhibits, and addenda hereto, constitutes the entire agreement between the parties with respect to its subject matter and supersedes all previous or contemporaneous agreements and understandings with respect to such subject matter.

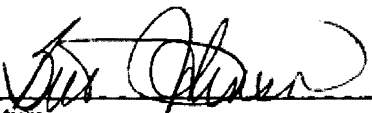
13.11. **Construction.** This Agreement may be amended only by a writing signed by an authorized representative of each party. If a term or provision of this Agreement is held invalid or unenforceable, the invalid term or provision will be amended to achieve as nearly as possible the same economic and operational effect as the original, and all other terms and provisions of this Agreement will remain in full force. Waiver by either party of a breach of any provision herein by the other party will not operate or be construed as a waiver of any subsequent, similar, or other breach. The captions and headings appearing herein are for reference only and will not be considered in construing this Agreement. As used in this Agreement, "including" means "including without limitation." Ambiguities shall be reasonably construed in accordance with all relevant circumstances, and shall not be construed against either party, irrespective of which party is deemed to have authored the ambiguous provision. The rights of each party granted herein are cumulative and are in addition to any others that a party is entitled to by law. This Agreement may be executed in any number of counterparts, each of which will be an original and all of which together will constitute one and the same instrument.

*// signature page follows //*

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives as of the Effective Date.

**Coordinated Care of Washington**

**SALISH BEHAVIORAL HEALTH  
ADMINISTRATIVE SERVICES  
ORGANIZATION, BY KITSAP  
COUNTY BOARD OF  
COMMISSIONERS, Its Administrative  
Entity**

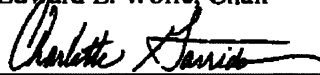
  
\_\_\_\_\_  
Signature

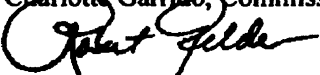
By: **Beth Johnson**  
\_\_\_\_\_  
**President & CEO**

Title: \_\_\_\_\_

Date: 8/15/19

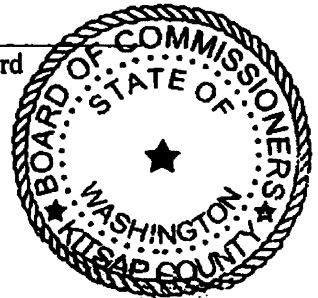
  
\_\_\_\_\_  
Edward E. Wolfe, Chair

  
\_\_\_\_\_  
Charlotte Garrido, Commissioner

  
\_\_\_\_\_  
Robert Gelder, Commissioner 8-12-19

ATTEST:

  
\_\_\_\_\_  
Dana Daniels, Clerk of the Board



**Attachment A**

**BENEFIT PLANS**

- **Apple Health Integrated Foster Care (IFC)**

**ATTACHMENT B**  
**ADMINISTRATIVE SERVICES**

BH-ASO shall provide the following Administrative Services to Plan under this Agreement:

**1. Services**

1.1. During the initial term specified in the Agreement, BH-ASO will provide the BH-ASO services necessary and sufficient for Plan ("Plan") to fulfill its obligations for "Crisis Service" provision as outlined in the IMC and IFC Contracts.

1.2. Per the IMC and IFC Contracts, this Agreement may be subject to HCA review and approval. BH-ASO and Plan agree to renegotiate this Agreement in good faith if required by HCA.

**2. Covered Programs**

2.1. BH-ASO's services apply to Plan's Members in the Salish Regional Service Area enrolled in the benefit plans listed in Attachment A.

**3. Covered Crisis Services**

3.1. BH-ASO shall provide the following Crisis Services under this Agreement. The services below align with those contractually obligated by the AH Contracts.

3.2. Per AH Contracts, crisis services shall be available twenty (24) hours per day, seven (7) days per week, three hundred sixty five (365) days per year. This shall include availability of a 24/7 regional crisis hotline that provides screening and referral to Plan's network of Participating Providers, where applicable, and availability of a 24/7 mobile crisis outreach team. Individuals will be able to access crisis services without full completion of intake evaluations and/or other screening and assessment processes. Crisis service codes shall include:

3.2.1. H0030

3.2.2. H2011

The Parties recognize and agree that the above list of codes may need to be amended based on the Parties' actual experience under the Agreement and therefore agree to meet and confer in good faith to discuss any changes that one Party requests.

3.3. Per the AH Contracts, BH-ASO and BH-ASO subcontractors shall collaborate with Plan to develop and implement strategies to coordinate care with community behavioral health providers for individuals with a history of frequent crisis system utilization.

3.4. For Plan members calling for crisis services who already receive WISE or PACT services, BH-ASO and/or its Subcontractor(s) will attempt to coordinate with existing case management support. Plan shall provide monthly reports to BH-ASO via sFTP of Plan members receiving WISE and PACT services.

3.5. Per the AH Contracts, BH-ASO will evaluate and monitor the performance of the crisis system and develop corrective action where needed. Examples of how this will occur may include, but are not limited to, the following:

3.5.1.1. Comparison of current and historical utilization that occurs after the effective date of this contract

3.5.2. Analysis of member and provider feedback.

#### **4. IT Implementation**

4.1.1. Per the AH Contracts, BH-ASO shall establish information systems to support data exchanges with the Plan, including, but not limited to eligibility interfaces, exchange of encounter data for crisis services paid for by BH-ASO, BH-ASO Participating Provider data, and sharing of care plans and mental health advance directive necessary to coordinate service delivery in accordance with applicable privacy laws, including HIPAA and 42 CFR Part 2. Encounter data exchange shall be guided by and comply with the requirements set forth in DBHR's Behavioral Health Data System (BHDS) Data Guide and Service Encounter Reporting Instructions (SERI) Guide.

4.1.2. For each transaction type noted above, BH-ASO will collaborate with the Plan to develop and obtain approval of all business requirement documents, conduct necessary end-to-end testing and establish agreed upon service level agreements (SLAs); these of which will become an amendment to this Agreement.

4.1.3. Per the AH Contracts, and based upon the defined/agreed upon business requirements, and completed acceptance testing performed by the Plan, BH-ASO will submit complete, accurate and timely encounter data to plan in formats prescribed by HCA, and in accordance with deadlines that Plan must adhere to in order to avoid financial penalties imposed by HCA. Plan will provide BH-ASO with applicable file format and submission schedule information.

4.1.4. BH-ASO will collaborate with the Plan to develop business requirements, technical specifications, conduct end-end testing and obtain Plan's approval prior to moving any system changes into its production systems.

4.2. Per of the AH Contracts, Plan shall make provisions for the BH-ASO to access a Member's individual service plan (or care plan) on a 24/7 basis for clients receiving Behavioral Health services, where applicable and with Member consent if required by law.

#### **5. Metrics and Monitoring**

5.1. BH-ASO will hold all of its subcontractors to the service level agreements and performance guarantees mandated by the HCA for handling of calls to the crisis line. BH-ASO will provide Plan with the service level targets as well as monthly reports of service level

**performance. BH-ASO will work with subcontractors to provide calls for audit upon Plan request.**

**ATTACHMENT C**  
**COMPENSATION DUE BH-ASO FOR ADMINISTRATIVE SERVICES**

Plan shall compensate BH-ASO as follows for BH-ASO's provision of the Administrative Services under this Agreement:

1. Plan shall pay to BH-ASO \$2.82 per Member per month (PMPM) for IFC members in consideration for the Behavioral Health Services for which BH-ASO arranges and the Administrative Services provided as set forth in Attachment B ("Monthly Payment"). BH-ASO shall be entitled to thirteen percent (13%) of the expenditures for the crisis services listed in Attachment B, for administrative costs. This 13% of administrative cost is included in the above stated PMPMs
2. Health Plan agrees to provide financial support to SBH-ASO for Ombuds Services to the Salish Regional Service Area Medicaid population. Health Plan's proportional share shall be based on the Health Plan's percentage of total Medicaid membership in the Salish Regional Service Area. The above stated administrative costs withheld from the PMPM is inclusive of Ombuds Services.
3. Plan shall pay the Monthly Payment to BH-ASO by electronic funds transfer on a monthly basis no later than the 7th day of the month, or business day following the 7th day of the month if the 7th day is a weekend or a federal holiday. The Administrative Fee shall be calculated based on the number of Members for the then current month included in the monthly eligibility file that Plan shall provide BH-ASO. Retroactive reconciliation based on member months shall be done as specified in this Agreement.
4. BH-ASO and MCO shall participate in financial reconciliation process, as directed by HCA, related to predicted versus actual Crisis Services utilization and fees and expense for direct services provided to MCO Members. Administrative fees will not be reconciled, unless otherwise directed by HCA. Reconciliation may result in the identification of an overpayment or underpayment by MCO to BH-ASO for the Covered Crisis Services provided under this Agreement. In the event there is a positive balance after reconciliation, such that MCO overpaid for Crisis Services, MCO reserves the right to reclaim that balance after the semi-annual reconciliation is completed. In the event there is a negative balance after reconciliation, BH-ASO reserves the right to request reimbursement of additional funds if the reconciliation shows the currently negotiated PMPM did not cover the costs of Member utilization of Crisis.
5. Per the BH-ASO Contract, BH-ASO shall submit claims and/or encounters for Covered Crisis Services consistent with the provisions of the BH-ASO Contract including, but not limited to Section 2.3, Billing Limitations.



Exhibit D  
BUSINESS ASSOCIATE AGREEMENT

This BUSINESS ASSOCIATE AGREEMENT ("*Agreement*") is entered into on this 1<sup>st</sup> day of January, 2020 (the "*Effective Date*") by and between Coordinated Care of Washington, Inc. and Coordinated Care Corporation for the benefit of themselves and their affiliates, (collectively, "*Covered Entity*") and Salish Behavioral Health Administrative Services Organization on behalf and for the benefit of itself and its affiliates ("*Business Associate*") (each, a "*Party*" and collectively, the "*Parties*").

WHEREAS, Covered Entity has affiliates (each, a Covered Entity "affiliate") that create, receive, transmit, maintain and/or disclose (collectively, "Use") "*Protected Health Information*" or "*PHI*" (as such terms are defined at 45 C.F.R. Section 164.500 et seq.), and Covered Entity and/or one or more of its affiliates desire to obtain services from Business Associate and/or the affiliates of Business Associate (each, a Business Associate "affiliate") that will result in the Use of such PHI by Business Associate and/or its affiliates pursuant to a contract (in effect as of, or after, the effective date of this Agreement) between Business Associate and/or any of its affiliates, on one hand, and Covered Entity and/or any of its affiliates, on the other hand (each contract, a "*Services Agreement*");

WHEREAS, irrespective of the Covered Entity affiliates and the Business Associate affiliates that are parties to any Services Agreement, Covered Entity and Business Associate desire this Agreement to govern the Use of all PHI by and between the Parties and their respective affiliates and to supersede all other agreements (including all other business associate agreements) between such entities regarding the Use of PHI; and

WHEREAS, pursuant to the authorities set forth above, Business Associate and its affiliates may Use PHI only in accordance with this Agreement.

NOW, THEREFORE, Covered Entity and Business Associate agree as follows:

1. Definitions.

1.1 The Health Insurance Portability and Accountability Act of 1996 ("*HIPAA*"), the Health Information Technology for Economic and Clinical Health Act ("*HITECH*"), and the implementing regulations thereunder, including but not limited to the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164 (the "*Privacy Rule*") and the Security Standards for the Protection of Electronic Health Information at 45 C.F.R. Parts 160 and 164 (the "*Security Rule*"), and the requirements of the final modifications to the HIPAA Privacy Rule, Security, Rule, et al., issued on January 25, 2013 and effective March 26, 2013, as may be amended from time to time, shall collectively be referred to herein as the "*HIPAA Authorities*." All other capitalized terms hereunder shall have the meaning ascribed to them elsewhere in this Agreement, or, if no such definition is specified herein, shall have the meaning set forth in the HIPAA Authorities.

1.2 "Affiliate" (capitalized or not) means any entity that controls, is controlled by or is under common control with a Party as well as any entity that is a subsidiary of an entity that controls a Party.

1.3 "Personally Identifiable Information" or "PII" shall include any data elements that identify an individual or that could be used to identify an individual, including but not limited to an individual's first name or initial and last name, all geographic subdivisions smaller than a state, all elements of dates (except year) for dates directly related to an individual including birth date, admission date, discharge date, date of death, telephone numbers, fax numbers, electronic mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers,

certificate or drivers license numbers, vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers, web universal resource locators (URLs), internet protocol (IP) address numbers, biometric identifiers, including finger and voice prints, full face photographic images and any comparable images; and any other unique identifying number, characteristic, code, or combination that allows identification of an individual.

1.4 "Protected Health Information" or "PHI" shall collectively refer to Protected Health Information, Electronic Protected Health Information ("ePHI"), each as defined by the HIPAA Authorities, and "Personal Identifiable Information" as defined above.

## 2. Interpretation of Provisions of this Agreement; Application of Agreement.

2.1 In the event of an inconsistency between the provisions of this Agreement and the mandatory terms of the HIPAA Authorities, the terms of the HIPAA Authorities shall prevail. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with the HIPAA Authorities. A reference in this Agreement to a section in the HIPAA Authorities means the section in effect or as amended. Titles or headings are used in this Agreement for reference only and shall not have any effect on the interpretation of this Agreement.

2.2 This Agreement governs the Use of all PHI that exists or arises in connection with a Services Agreement irrespective of the Covered Entity affiliate and Business Associate affiliate that may be parties to such Services Agreement. Each Party hereto represents and warrants that (i) it is validly existing under the laws of the state of its formation; (ii) it has the full right, authority, capacity and ability to enter into this Agreement for the benefit and, in the case of Business Associate, on the behalf of. itself and each of its affiliates and to carry out its and its affiliates' obligations hereunder; (iii) this Agreement is a legal and valid obligation binding upon it and it shall cause all of its affiliates that Use PHI pursuant to a Services Agreement to comply with the obligations hereunder of such Party; and (iv) its execution, delivery and performance of this Agreement does not conflict with any agreement, instrument, obligation or understanding to which it or any of its affiliates are bound.

## 3. Obligations of Business Associate.

3.1 Limits on Use and Disclosure. Business Associate agrees to not use or further disclose PHI other than as permitted by this Agreement or as Required by Law. Business Associate further agrees that to the extent it is carrying out one or more of the Covered Entity's obligations under the Privacy Rule, it shall comply with the requirements of the Privacy Rule that apply to the Covered Entity in the performance of such obligations.

3.2 Safeguards. Business Associate agrees to use reasonable and appropriate administrative, physical and technical safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement. More specifically, as also provided for in Section 3.12 below, Business Associate agrees to establish, implement and maintain appropriate safeguards, and comply with the Security Rule with respect to Electronic PHI, as necessary to prevent any use or disclosure of PHI other than as provided for by this Agreement.

3.3 Mitigation of Harm. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement or the HIPAA Authorities and shall take prompt steps to prevent the recurrence of any Incident, including any action required by applicable federal and state laws and regulations. All such efforts will be subject to Covered Entity's prior written approval. In the event of an Incident (as defined below), Business Associate shall promptly develop and provide to Covered Entity a written correction action plan which describes the measures to be taken to halt and/or contain such Incident.

3.4 **Report of Improper Use or Disclosure.** "Incident" means (i) any successful Security Incident, (ii) Breach of Unsecured PHI, or (iii) any loss, destruction, alteration or other event in which PHI cannot be accounted for. Successful Security Incidents shall not include pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI. Business Associate agrees to notify Covered Entity, in writing immediately upon discovery, but not later than the same day of discovery of any Incident (by Business Associate or by a Subcontractor) involving the acquisition, access, use or disclosure of the PHI not provided for by this Agreement of which Business Associate becomes aware. As soon as reasonably possible thereafter, in no case more than seven (7) calendar days following discovery of the Incident, Business Associate shall provide Covered Entity with a written report which shall include but not be limited to: i) a description of the circumstances under which the Incident occurred; ii) the date of the Incident and the date that the Incident was discovered; iii) a description of the types of PHI involved in the Incident; iv) the identification of each Individual whose PHI is known or is reasonably believed by the Business Associate to have been affected; and v) any recommendations that the Business Associate may have, if any, regarding the steps that Individuals may take to protect themselves from harm. To the extent that Covered Entity reasonably determines that such Incident necessitates the notification of Individuals by Covered Entity under HITECH, Business Associate agrees that it shall immediately reimburse Covered Entity for the reasonable expenses of such notification process. Business Associate shall cooperate with any investigation (and/or risk assessment) of such Incident conducted by Covered Entity in connection with any report made pursuant to this Section. Business Associate shall make itself and any subcontractors and agents assisting Business Associate in the performance of its obligations available to Covered Entity to testify as witnesses, or otherwise, in the event of an Incident.

3.5 **Subcontractors.**

(a) Prior to the date on which any Subcontractor (including any affiliate that is a Subcontractor) creates, receives, maintains or transmits PHI on behalf of Business Associate in connection with Business Associate's obligations under the Services Agreement, Business Associate agrees to enter into a written agreement with any Subcontractor ("*Subcontractor Agreement*") to whom Business Associate provides PHI that requires them: (i) to comply with the same HIPAA Authorities that apply to Business Associate under the Agreement; and (ii) to comply with the same restrictions and conditions that apply to Business Associate through this Agreement with respect to such PHI.

(b) Upon Business Associate's knowledge of a material breach of the Subcontractor Agreement by Subcontractor, Business Associate shall immediately notify Covered Entity of such material breach in writing and, at its option (unless otherwise directed by Covered Entity), shall: **(i) provide an opportunity for Subcontractor to cure the breach or end the violation and terminate this Agreement if Subcontractor does not cure the breach or end the violation within the cure period identified in the Services Agreement between Covered Entity and Business Associate, or if no cure period is identified in the Services Agreement, as specified by Covered Entity; (ii) immediately terminate this Agreement if Subcontractor has breached a material term of this Agreement and Business Associate (or Covered Entity) deems cure by the Subcontractor not to be possible; or (iii) if neither termination nor cure are feasible, report the violation to the Covered Entity.**

(c) Business Associate agrees to provide Covered Entity with a list of any and all such Subcontractors and, in the event of an Incident, employees that create, receive, maintain or transmit PHI on behalf of Business Associate in connection with Business Associate's obligations under the Service Agreement with Covered Entity within thirty (30) days of such a request.

3.6 **Access to Records.** At the request of Covered Entity and within five (5) business days of such request and in a reasonable manner designated by Covered Entity, Business Associate shall provide access to PHI in a Designated Record Set to Covered Entity or, as directed by Covered Entity, to an

Individual, in a manner compliance with 45 CFR §164.524 and/or other applicable provisions of the HIPAA Authorities.

3.7 Amendments to PHI. At the request of Covered Entity, or, as directed by Covered Entity, at the request of an Individual, Business Associate shall make, within five (5) business days of such request and in a reasonable manner designated by Covered Entity, any amendment(s) to PHI in a Designated Record Set to which the Covered Entity has agreed pursuant to 45 CFR §164.526, or shall otherwise assist Covered Entity in complying with Covered Entity's obligations under 45 CFR §164.526.

3.8 Availability of Internal Practices, Books and Records. Business Associate shall make its internal practices, books and records available to Covered Entity or the Secretary for purposes of determining Covered Entity's compliance with the HIPAA Authorities, in a time and manner designated by Covered Entity or the Secretary, as applicable. Covered Entity reserves the right to request, and Business Associate shall provide, additional satisfactory assurances that Business Associate is meeting its applicable obligations under the HIPAA Privacy and Security Rules. Such requests may include, but are not limited to; an onsite audit, conducted by Covered Entity or its designee, access to policies and procedures, risk assessment documentation, incident logs or information related to the Business Associate's Subcontractors compliance with their applicable obligations under the HIPAA Privacy and Security Rules.

3.9 Accounting of Disclosures. Business Associate shall document such disclosures of PHI and information related to such disclosures (i.e., (i) the date of the disclosure; (ii) the name of the entity or person who received the PHI and, if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably states the basis for the disclosure) as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR §164.528. Such documentation shall be maintained with regard to all disclosures of PHI, except for those disclosures that are expressly exempted from the documentation requirement under the HIPAA Authorities (see, e.g., 45 CFR §§164.502; 164.508; 164.510; 164.512, etc.). Documentation required to be collected by the Business Associate under this Section shall be retained for a minimum of six (6) years, unless otherwise provided under the HIPAA Authorities. Business Associate shall further provide the information collected pursuant to this Section to Covered Entity or an Individual, within five (5) business days of the applicable request and in a reasonable manner designated by Covered Entity, as necessary to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR §164.528 or other applicable provision of the HIPAA Authorities.

3.10 Disclosure of Minimum PHI. Business Associate agrees that it shall request, use and/or disclose only the amount and content of PHI that is the Minimum Necessary for Business Associate to fulfill its obligations under the terms and conditions of this Agreement. Business Associate acknowledges that such Minimum Necessary standard shall apply with respect to uses and disclosures by and among members of Business Associate's workforce as well as by or to third parties as permitted hereunder.

3.11 Notification of Claims. Business Associate shall promptly notify Covered Entity upon notification or receipt of any civil or criminal claims, demands, causes of action, lawsuits, or governmental enforcement actions ("*Actions*") arising out of or related to this Agreement or PHI, or relating to Business Associate's conduct or status as a business associate for any covered entity, regardless of whether Covered Entity and/or Business Associate are named as parties to such Actions.

3.12 Security Rule Requirements. Business Associate shall implement Administrative, Physical, and Technical Safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic PHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity as required by the Security Rule. Additionally, Business Associate shall comply with the Security

& Privacy Requirements described in the attached Security & Privacy Addendum. Not more than once per calendar year, Business Associate shall within ten (10) days after request from Covered Entity truthfully complete and duly execute the Annual Attestation that is attached hereto or, alternatively, notify Covered Entity in writing of any facts or events that would render untrue any statement within the Annual Attestation. Business Associate shall document policies and procedures that implement the foregoing requirements and shall, upon request, provide them to Covered Entity, who may further disclose them to any governmental entity with regulatory oversight over Covered Entity. Business Associate agrees to report to Covered Entity any use or disclosure of PHI not provided for by this Agreement or the HIPAA Authorities of which it becomes aware, including any Incident. Accordingly, as also provided in Section 3.4, Business Associate agrees to report any Incident of which it becomes aware to Covered Entity immediately, but not later than the same day of discovery of the Incident. All reports required of the Business Associate pursuant to this Section shall be provided as specified in Section 3.4 of this Agreement, including the actions and the mitigation steps, if any, taken by Business Associate in response to the Incident(s).

3.13 Compliance with HIPAA Authorities. Requirements of the HIPAA Authorities that are made applicable with respect to business associates, or any other provision required to be included in this Agreement pursuant to the HIPAA Authorities, are incorporated into this Agreement by this reference.

#### 4. Permitted Uses and Disclosures by Business Associate.

4.1 Use or Disclosure to Perform Functions, Activities, or Services. Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to perform those functions, activities, or services that Business Associate performs for, or on behalf of, Covered Entity as specified in the Services Agreement, provided that such use or disclosure would not violate the Privacy Rule, or the policies and procedures of Covered Entity relating to the "Minimum Necessary Standard," if done by Covered Entity. Any such use or disclosure shall be limited to those reasons and those Individuals as necessary to meet the Business Associate's obligations under the Services Agreement.

4.2 Appropriate Uses of PHI. Except as may be otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

4.3 Confidentiality Assurances and Notification. Except as may be otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are Required by Law, or Business Associate obtains reasonable assurances from the person to whom the PHI is disclosed that such PHI will remain confidential and used or further disclosed only as Required by Law or for the purpose for which such PHI was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached.

4.4 Data Aggregation Services. As applicable, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 42 CFR § 164.504(e)(2)(i)(B), except as may be otherwise provided by this Agreement.

5. Indemnification. Each party (the "*Indemnitor*") shall indemnify and hold harmless the other party (the "*Indemnitee*") against, and reimburse such Indemnitee for, any expense, loss, damages, fees, costs, claims or liabilities of any kind arising out of or related to any Actions asserted or threatened by a third party arising out of or related to the Indemnitor's acts and omissions associated with its obligations under this Agreement or its use or disclosure of PHI or, when the Indemnitor is the Business Associate, the

Use of PHI by a Subcontractor or affiliate of Business Associate. Such indemnification shall include, but not be limited to, the payment of all reasonable attorney fees associated with any such Action.

**6. Obligations of Covered Entity.**

6.1 Notice of Privacy Practices. Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's notice of privacy practices, to the extent that such limitation(s) may affect Business Associate's use or disclosure of PHI.

6.2 Change or Revocation of Permission. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's permitted or required uses and disclosures of PHI. Business Associate shall comply with any such changes or revocations.

6.3 Restrictions on Use or Disclosure. Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent such restriction may affect Business Associate's use or disclosure of PHI. Business Associate shall comply with any such restrictions. Business Associate shall immediately notify Covered Entity of any request for a restriction on the use or disclosure of an Individual's PHI that Business Associate receives from such Individual.

6.4 No Request to Use or Disclose in Impermissible Manner. Except as necessary for the Data Aggregation Services or management and administrative activities of the Business Associate as allowed herein, Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

**7. Term and Termination**

7.1 Term. This Agreement shall be effective as of the earlier of the date first documented above or the effective date of the Services Agreement, and shall terminate upon termination of the Services Agreement for any reason or as otherwise provided in this Agreement.

7.2 Termination with Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, or its Subcontractors, Covered Entity shall, at its option: (i) provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within the cure period identified in the Services Agreement, or if no cure period is identified in the Services Agreement, as specified by Covered Entity; (ii) immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and Covered Entity deems cure by Business Associate not to be possible; or (iii) if neither termination nor cure are feasible, report the violation to the Secretary.

**7.3 Effect of Termination.**

(a) Except as provided in paragraph 7.3(b) of this Section, upon termination of this Agreement for any reason, Business Associate shall return or destroy (at Covered Entity's election), and shall retain no copies of, all PHI in the possession of Business Associate.

(b) In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity written notification of the conditions that make return or destruction infeasible. Upon Covered Entity's written approval, which shall not be

unreasonably withheld, Business Associate may retain the PHI, but shall extend the protections of this Agreement (including, but not limited to, Sections 1 through 5) 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 Business Associate maintains such PHI.

8. **Standards for Electronic Transactions.** In connection with the Services to be provided to Covered Entity pursuant to this Agreement, Business Associate agrees that if it (or a Subcontractor) conducts an electronic transmission for which the Secretary has established a "standard transaction" under 45 C.F.R. Part 164, Subparts A, C, D and E, as applicable (the "*Electronic Transactions Standards*"), Business Associate (or its Subcontractor) shall comply with the requirements of the Electronic Transactions Standards. Business Associate specifically represents that it has obtained such compliance. Business Associate agrees that, in connection with the transmission of standard transactions, it will not (and will not permit any Subcontractor with which it might contract to): (i) change the definition, data condition, or use of a data element in a standard; (ii) add any data elements or segments to the maximum defined data set; (iii) use any code or data elements that are either marked "not used" in the standard's implementation specification or are not in the standard's implementation specification; or (iv) change the meaning or intent of the standard's implementation specification(s). Business Associate understands that Covered Entity reserves the right to request an exception from the uses of a standard as permitted by 45 CFR § 162.940, and, if such an exception is sought, Business Associate agrees to participate in a test modification.

9. **Confidentiality of Business Information.**

9.1 **Business Information.** In the event the parties have not agreed to alternative confidentiality language with respect to business information in the Services Agreement or elsewhere, the following provisions will apply. Neither party will disclose to any third party any information related to this Agreement or to the business operations of the other party, or any proprietary information belonging to the other party (collectively, "*Confidential Business Information*") without the prior written consent of the other party, except as may be required under law or this Agreement; provided that a party required by law to disclose Confidential Business Information shall inform the other party in order that the other party may contest such requirement. Each party hereby agrees that all Confidential Business Information communicated to it by the other party, whether oral or written, and whether before or after execution of this Agreement, was and will be received in strict confidence and will be used only for purposes set forth in the Services Agreement. Upon termination of this Agreement, each party shall, upon the request of the providing party, promptly return all such Confidential Business Information to the providing party or, at the providing party's option, shall destroy such Confidential Business Information and certify as to its destruction, except that each party shall be permitted to retain copies of Confidential Business Information as is reasonably necessary for its internal compliance and auditing purposes, provided the terms of this Section 9 shall continue to apply with respect to such retained Confidential Business Information for so long as it is retained. This obligation of confidentiality shall not apply to information i) which was known by the recipient without the obligation of confidentiality prior to its receipt of such information; ii) is or becomes publicly available without breach of this Agreement; or iii) is received from a third party without an obligation of confidentiality and without breach of this Agreement. This paragraph shall not apply to uses and disclosures of PHI, which shall be governed by the remaining provisions of this Agreement.

9.2 **Response to Subpoena.** Business Associate shall be permitted to disclose PHI and Confidential Business Information that Business Associate is required to disclose pursuant to court order, subpoena or other compulsory legal process, provided that prior to making any disclosure thereunder, Business Associate shall provide Covered Entity within five (5) calendar days prior written notice (or as much notice as reasonably practicable under the circumstances) of the intended disclosure, specifying the basis and nature of the same.

10. **Miscellaneous.**

10.1 **Assignment; Waiver.** This Agreement shall be binding upon and inure to the benefit of the respective legal successors of the parties. Neither this Agreement nor any rights or obligations hereunder may be assigned, in whole or in part, without the prior written consent of the other party. Except as provided herein, this Agreement shall create no independent rights in any third party or make any third party a beneficiary hereof. No failure or delay by either party in exercising its rights under this Agreement shall operate as a waiver of such rights, or of any prior, concurrent, or subsequent breach.

10.2 **Property Rights.** All PHI shall be and remain the exclusive property of Covered Entity. Business Associate agrees that it acquires no title or rights to the PHI, including any de-identified information, as a result of this Agreement.

10.3 **Right to Cure.** Business Associate agrees that in the event Business Associate fails to cure a breach of this Agreement pursuant to this Agreement, Covered Entity has the right, but not the obligation, to cure the same. Expenses, costs or fines reasonably incurred in connection with Covered Entity's cure of Business Associate's breach(es) shall be borne solely by Business Associate.

10.4 **Injunctive Relief.** Business Associate agrees that breach of the terms and conditions of this Agreement shall cause irreparable harm for which there exists no adequate remedy at law. Covered Entity retains all rights to seek injunctive relief to prevent or stop any breach of the terms of this Agreement, including but not limited to the unauthorized use or disclosure of PHI by Business Associate or any Subcontractor, contractor or third party that received PHI from Business Associate.

10.5 **Survival; Severability.** The respective rights and obligations of Business Associate under this Agreement, including but not limited to Business Associate's indemnification obligations, shall survive the termination of this Agreement. The parties agree that if a court determines that any of the provisions of this Agreement are invalid or unenforceable for any reason, such determination shall not affect the enforceability or validity of the remaining provisions of this Agreement.

10.6 **Entire Agreement; Amendment.** This document, together with any written Schedules, amendments and addenda, constitutes the entire agreement of the parties and supersedes all prior oral and written agreements or understandings between them with respect to the matters provided for herein. The parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity and Business Associate to comply with the requirements of the HIPAA Authorities. Any modifications to this Agreement shall be valid only if such modifications are in accordance with the HIPAA Authorities, are made in writing, and are signed by a duly authorized agent of both parties.

10.7 **Governing Law.** This Agreement shall be governed by and construed in accordance with the laws of the State of Washington to the extent that the HIPAA Authorities do not preempt the same.



**10.8 Notice.** Any notice required or permitted to be given by either party under this Agreement shall be sufficient if in writing and hand delivered (including delivery by courier) or sent by postage prepaid certified mail return receipt requested, to the following address:

**If Covered Entity:**

Name: Sheila Nishimoto  
Title: VP, Compliance  
Company: Coordinated Care  
Address: 1145 Broadway, Suite 300  
Tacoma, WA 98402  
Phone: (877) 644 4613

**If Business Associate:**

Name: Edward E. Wolfe  
Title: Chair, Kitsap County  
Company: Salish Behavioral Health-ASO  
Address: 614-Division Street, MS-23  
Port Orchard, WA 98366  
Phone: 800-525-5637

**10.9 Independent Contractors.** For purposes of this Agreement, Covered Entity and Business Associate, and Covered Entity and any Subcontractor of Business Associate, are and will act at all times as independent contractors. None of the provisions of this Agreement shall establish or be deemed or construed to establish any partnership, agency, employment agreement or joint venture between the parties. Each party to this Agreement warrants that it has full power and authority to enter into this Agreement, and the person signing this Agreement on behalf of either party warrants that he/she has been duly authorized and empowered to enter into this Agreement.

**COVERED ENTITY**

By: [Signature]  
Title: President & CEO  
Date: 8/15/19

**BUSINESS ASSOCIATE**

By: [Signature]  
Title: Chair, Kitsap County  
Date: 8-12-19

## **SECURITY & PRIVACY ADDENDUM**

### **Business Continuity, Enterprise Resilience, and Disaster Recovery**

1. **Business Impact Analysis:**
  - a) **Critical IT systems and components must be identified and documented, including recovery time objective and recovery point objective.**
2. **Recovery Strategies**
  - a) **The data center must maintain a back-up site(s).**
  - b) **Mission critical information must be fully backed-up on a weekly basis and incrementally changes must be backed up daily.**
  - c) **Backed-up information must be stored encrypted with FIPS 140-2 compliant encryption protocols.**
  - d) **Backed-up information must be stored in a secure off-site facility.**
  - e) **Backed-up information must be stored off-line.**
  - f) **Restoration of critical data back-ups must be no less semi-annually (every 6 months).**
  - g) **Contracts for outsourced services must include disaster recovery agreements.**
3. **Recovery Plans and Procedures, and Maintenance**
  - a) **A documented business continuity plan for business functions must be updated and maintained.**
  - b) **The business continuity plan must be stored off-site in a secure location.**
  - c) **Centene must be alerted of any deficiencies discovered in the business continuity plan that would adversely affect Centene.**
  - d) **A documented disaster recovery plan for information technology must be updated and maintained.**
  - e) **The disaster recovery plan must be stored off-site in a secure location.**
  - f) **The disaster recovery plan must include policies and procedures for facility access during a disaster.**
4. **Testing and Exercising**
  - a) **The business continuity plan for business functions must be tested periodically.**
  - b) **The disaster recovery plan for information technology must be tested periodically.**

## **5. Escalation and Crisis Management**

- a) The business continuity plan must contain notification procedures to alert Centene of service disruptions including off-hour and weekend coverage.
- b) The disaster recovery plan must have notification procedures to alert Centene of service disruptions including off-hour and weekend coverage.

## **IT Risk and Compliance Management**

### **1. Regulatory and Standards Implementation**

- a) The Company must remain in compliance with HIPAA and all other applicable national and state privacy and security regulations.
- b) Confidential information, including PHI and ePHI, must never be stored outside of the United States.
- c) An information security officer must be assigned.
- d) An on-going and documented security awareness program must be established and communicated to all users to make them aware of the confidentiality of information, the company's security policies, standards, and good security practices.
- e) Information Security awareness information must be distributed to all users on a periodic basis.
- f) A privacy officer must be assigned.
- g) An on-going and documented privacy awareness program must be established and communicated to all users to make them aware of the company's privacy policies and the requirements to protect the confidentiality of information.
- h) Privacy awareness information must be distributed to all users on a periodic basis.
- i) Mandatory privacy training must be delivered to, managed, and validated for all users on no less than an annual periodic basis.
- j) All users are required to sign confidentiality and non-disclosure agreements.

### **2. Risk and Compliance Assessments**

- a) An accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of confidential information, including PHI and ePHI is conducted at least annually.
- b) All users are required to have a national criminal background check, a local court background check for the past seven (7) years and a financial background check.

### **3. Policies, Standards, and Procedure Management**

- a) A documented risk management function and/or program supported by executive management must exist.
- b) A documented information security function and/or program supported by executive management must exist.
- c) A documented privacy function and/or program supported by executive management must exist.
- d) The information security function/program must establish security policies and standards that are enforced through automated systems and administrative procedures that are maintained and updated as needed.
- e) The privacy function/program must establish confidentiality policies which are maintained and updated as needed.

#### 4. Issue and Corrective Action Management

- a) Controls are implemented to reduce risks and vulnerabilities to a reasonable and appropriate level
- b) A documented process must exist and be adhered to in order to report security issues affecting Centene to Centene's Information Security Officer.
- c) A documented process must exist and be adhered to in order to report privacy issues affecting Centene PHI and ePHI to Centene's Privacy Officer.

#### 5. Exception Management

- a) Disciplinary measures for violations must be included in the Information Security and Privacy Program.
- b) A documented security incident response plan must exist to ensure incidents are tracked, monitored, and investigated until closure is achieved.
- c) A documented privacy incident response plan must exist to ensure that incidents are tracked, monitored, investigated and reported internally and to Covered Entity until remediation and closure is achieved.

### **Data Protection**

#### 1. Data Classification & Inventory

- a) A documented information classification scheme must be utilized to ensure proper protection, use and destruction of Centene's data.

#### 2. Data Lifecycle Analysis

- a) Systems containing confidential information, including PHI and ePHI, have been documented, including security and privacy controls.

- b) Documents showing the flow of sensitive data through systems and business processes must exist.

### 3. Data Encryption & Obfuscation

- a) Confidential information, including PHI and ePHI, must be encrypted during storage on all devices including handhelds, laptops, workstations, and removable media with FIPS 140-2 compliant encryption protocols.
- b) Information containing PHI and ePHI must be encrypted during storage on servers with FIPS 140-2 compliant encryption protocols.
- c) Confidential information, including PHI and ePHI, must be encrypted during transmission over public or untrusted networks, including wireless or email transmissions, with FIPS 140-2 compliant encryption protocols.
- d) Business to business communications with confidential information, including PHI and ePHI, must be encrypted.

### 4. Data Loss Prevention

- a) A documented policy and process must exist with regard to the removal or movement of confidential information, including PHI and ePHI to unsecured systems or media.
- b) Confidential information, including PHI and ePHI, stored on removable media must be secured with restricted access to those with a business need.
- c) Technical controls must exist to prevent transmission of confidential information, including PHI and ePHI to unauthorized recipients.
- d) Technical controls must exist to prevent storage of confidential information, including PHI and ePHI, on unsecured systems.

### 5. Data Retention and Destruction

- a) A documented policy and process must exist with regard to the removal or destruction of confidential information, including PHI and ePHI. When appropriate, confidential information, including PHI and ePHI, must be purged or destroyed using a NIST 800-88 approved process when no longer needed.

## **Third Party Risk Management**

### 1. Evaluation & Selection

- a) A documented process must exist to evaluate the privacy and security controls for the Company's agents, subcontractors and outsourced services prior to entering into any such approved subcontracts.

### 2. Contract & Service Initiation

- a) Any subcontracts shall contain all privacy and security requirements and protections as set forth in this Security Addendum.
- b) Information containing PHI or ePHI must only be disclosed to third parties when a Business Associate Agreement (BAA) and non-disclosure agreement are in effect.

### 3. Security & Compliance Review

- a) A documented process exists to review the privacy and security controls of agents, subcontractors and outsources services on a periodic basis to reasonably assure they are maintaining the required level of protection.

### 4. Third Party Monitoring

- a) Agents, subcontractors, and outsourced services that perform critical services that support this contract have been identified and documented.
- b) Agents, subcontractors, and outsourced services that are identified as providing critical services or that are handling PHI must be monitored on an ongoing basis for contract compliance.

## **Identity & Access Management**

### 1. User Account Management

- a) Access to systems and applications must require a unique identifier (e.g. user ID) and at minimum a password or equivalent control.
- b) User IDs must be locked after 5 consecutive unsuccessful login attempts.
- c) User IDs must be disabled after 60 days or less of inactivity.
- d) Passwords must be issued to users in a secure manner and be changed at first login.
- e) Password policies at a minimum must include minimum password length, alphanumeric composition, retention of password history, and password change frequency.
- f) Passwords cannot be displayed on screens or on reports.
- g) Passwords must be encrypted in transmission and storage.

### 2. Access Management

- a) Access to confidential information, including PHI and ePHI, must be restricted to individuals that have a business need and access control mechanisms must be implemented that limit access to confidential information.
- b) Security administration procedures must include procedures for access requests for a new user, changing access, prompt deletion of users involving terminations, user transfers and periodic verification of users and access rights.

- c) All user access requests must be documented with management approval including privileged users.
- d) Documented remote access policies must exist and be enforced.

### 3. Privileged User Management

- a) All default supplied user IDs must be disabled, renamed, or deleted wherever possible.
- b) System IDs must be documented describing their functions and risks.
- c) System IDs must be required to have passwords and documented risk analysis if password change frequency is not enforced.
- d) System ID passwords must be stored in encrypted files.
- e) System IDs are not allowed to be scripted into the application.
- f) System IDs must not be able to be accessed by an individual user for interactive use.
- g) All vendor-supplied default passwords must be changed.

### 4. Data Platform Integration

- a) All systems containing confidential information, including PHI and ePHI, have system access controls to prevent unauthorized disclosure or modification.
- b) Single sign on technologies are leveraged wherever possible to eliminate the need for multiple access controls systems.

### 5. Access Reporting and Audit

- a) All user access to systems containing confidential data, including PHI and ePHI, must be revalidated at least annually.
- b) All User IDs and System IDs with privileged authorities must be revalidated at least quarterly.

### 6. Access Governance

- a) User access must be defined by job roles to ensure segregation of duties.
- b) User access must be logged and tracked to an individual for accountability.

### 7. Federation

- a) Access to systems by agents, subcontractors, or outsourced services are subject to the same Identity Management requirements as Company personnel.

## **Secure Development Lifecycle**

- 1. Security and Risk Requirements**
  - a) A documented process exists to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of confidential information, including PHI and ePHI, as part of the System Development Life Cycle.
  - b) Security controls are considered throughout the System Development Life Cycle.
- 2. Security Design & Architecture**
  - a) Security controls are designed to eliminate a single point of failure.
  - b) Systems are designed to use a common security architecture.
  - c) Production, test, and development environments must be physically and/or logically separated.
- 3. Application Role Design and Access Privileges**
  - a) Application security controls are designed to ensure users can access only information for which they have an authorized business need.
  - b) Access is controlled by a common access methodology or single sign on wherever feasible.
- 4. Secure Coding Guidelines**
  - a) Secure coding principles and practices are documented and followed.
  - b) Web application controls must be configured to prevent printing or downloading data to unauthorized workstation and/or mobile devices.
  - c) Production information must not be used in development and test environments unless such environments are secured to the same level as production, or data has been de-identified as specified in HIPAA (45 CFR 164.514).
- 5. Secure Build**
  - a) New server and network equipment deployment procedures must ensure implementation of security configuration settings.
- 6. Security Testing**
  - a) All security controls must be tested prior to implementing new systems or upgrades into production.
  - b) Where feasible, automated tools are used for code review.
- 7. Roll-out and Go-live Management**



- a) Staff other than developers are responsible for moving systems or applications into production environment to retain separation of duties.
- b) All non-standard access paths are removed prior to move into production.

**8. Application Security Administration**

- a) Development staff requires management approval to access production systems.
- b) Technical staff must not have access to production data, programs, or applications unless required to perform their jobs.

**Infrastructure, Operations and Network Security/Cyber Threat and Vulnerability Management**

**1. Antivirus (AV) & Malware protection**

- a) A documented policy and procedures exist for guarding against, detecting, and reporting malicious software.

**2. Intrusion Detection and Prevention**

- a) Intrusion detection and prevention systems must be implemented for critical components of the network.

**3. Network Access Controls**

- a) A documented policy and procedures exist to prevent unauthorized/unsecured devices from accessing the network.

**4. Network and Application Firewalls**

- a) Firewalls must be implemented and configured to deny all except authorized documented business services.
- b) Firewalls must be configured to fail in a prevent state.

**5. Proxy/Content Filtering**

- a) A documented policy and procedures exist to prevent confidential information, including PHI and ePHI, from being transmitted to unauthorized recipients or stored in unauthorized locations.

**6. Remote Access Controls**

- a) Two-factor authentication is implemented for all remote network access (e.g. VPN, Citrix, etc.).

**7. Security Monitoring**

- a) A documented policy and procedures exist to monitor networks, systems, and applications for potential security events.

- b) A documented process exists to respond to potential security events on a 24x7x365 basis.
- c) All significant computer security relevant events must be securely logged.
- d) Computer systems handling confidential information, including PHI and ePHI, must securely log all significant computer security relevant events including the following: (a) unauthorized attempts to enter the system, (b) unauthorized attempts to access protected information or resources, (c) all attempts to issue restricted commands, (d) security activities, (e) special privileged user activities and (f) violation activities.
- e) All logs of computer security relevant events must be traceable to specific individuals wherever possible.

#### **8. Wireless Security Controls**

- a) A documented policy and procedures exist to prevent unauthorized wireless access to production systems.

#### **9. Database Security**

- a) A documented policy and procedures exist to prevent unauthorized updates to databases.
- b) All database access must be traceable to specific individuals.

#### **10. Network Device Security**

- a) All network devices supporting business critical systems have physical and logical access controls.
- b) All network devices supporting business critical systems have secured out-of-band management.

### **Cyber Threat and Vulnerability Management**

#### **1. OS Hardening & Secure Configuration**

- a) Required security configuration settings must be selected and documented.
- b) Documented processes must exist to periodically verify security configuration settings.
- c) Any and all Workstations able to access any confidential information must actively and automatically blank the screen or enable a screen saver and require re-authentication after fifteen (15) minutes of inactivity or less.

#### **2. Patch Management**

- a) A documented patch management process must exist and be enforced.
- b) Prompt application of security patches, service packs, & hot fixes is required for all systems that store, process, manage, or control access to sensitive data, including PHI and ePHI.

### **3. Vulnerability Management**

- a) A documented process and procedures exist to identify, quantify, prioritize, track, and remediate vulnerabilities.

### **4. Recurring Vulnerability Assessments and Penetration Testing**

- a) Periodic third party penetration tests must be conducted from outside and within the network.
- b) Vulnerability assessment must be performed at least quarterly.

### **5. Incident and Problem Management**

- a) A documented problem management system must exist.
- b) Audit logs must be implemented on all systems storing or processing critical or confidential information.
- c) Audit logs must be retained for a minimum of twelve (12) months.
- d) Audit logs must be protected from unauthorized access and resistant to attacks including deactivation, modification or deletion.
- e) Audit logs must be reviewed for inappropriate activities in a timely manner and appropriate actions must be taken to protect Centene associates, assets, systems, and data.

### **6. Capacity Management**

- a) A documented policy and process exists to evaluate current capacity against projected requirements.

### **7. Configuration and Change Management**

- a) A three-tiered architecture must be deployed to isolate web applications from production information in the "internal" network.

### **8. Release Management**

- a) Segregation of duties between change management, developer, and infrastructure staff must be maintained.

Developers must not be able to update production resources without proper change management procedures for production updates/fixes.

- b) All production systems and application resources must be changed through an enforced and documented change management process which includes appropriate reviews, testing, and management approvals.
- c) Production code and systems must not allow undocumented changes or updates.

## **9. Asset and Configuration Management**

1. Documented network diagrams must exist.
2. An auditable and documented inventory of information technology assets must exist in case of loss or theft.

## **Physical Security**

### **1. Policies, Standards, and Procedure Management**

- a) A documented physical security function and/or program must exist.
- b) The physical security function/program must establish physical security policies and be enforced through automated systems and administrative procedures.
- c) All servers storing or processing confidential information, including PHI and ePHI, must be located in a secure data center or equivalent secure facility.

### **2. Facility Access Controls**

- a) Employees must be required to wear identification badges at all times in sensitive facilities.
- b) Visitors must be required to be identified, sign in, wear temporary visitor badges, and be escorted in facilities containing Centene data.
- c) Data center access to sensitive areas, such as a computer room, must require two levels of authentication.
- d) Data center and other sensitive facilities access must be periodically reviewed to ensure that access is still valid.
- e) Facility access logs must be retained for at least six (6) months and be reviewed as needed.

### **3. Issue and Corrective Action Management**

- a) Any known HIGH risk physical security vulnerabilities affecting Centene must be communicated to Centene's Corporate Information Security Officer.
- b) The Data Center facility must be equipped and maintained with fire detection/suppression, surge and brown-out, air conditioning, and other computing environment protection systems necessary to assure continued service for critical computer systems.
- c) Policies and procedures must be in place to document repairs and modifications to physical components of facilities where PHI and ePHI are stored, which are related to security (for example, hardware, walls, doors and locks).
- d) All hardware and electronic media containing PHI and ePHI must be identified and tracked during movement.

- e) A retrievable exact copy of PHI and ePHI must be created from equipment before being moved.

**Changes**

Centene may change the above security requirements by providing new requirements in writing to Business Associate. Business Associate shall comply with such new security requirements within thirty (30) days after receipt of notice. In the event Business Associate's compliance with the new requirements materially increases its cost to provide services under the Services Agreement(s), Business Associate shall notify Centene of the amount Business Associate believes is necessary to reimburse Business Associate for its actual and reasonable additional costs. If Centene elects not to reimburse Business Associate for such costs, then Centene may terminate this Agreement and/or any or all of the Services Agreements, in whole or in part, by sending written notice to Business Associate indicating which Services Agreements are being terminated and the effective date of termination. Such termination shall be without charge to Centene, except that Centene shall pay for all services under such terminated contract(s) that were properly rendered until the effective date of termination.

\*\*\*\*\*

**ANNUAL ATTESTATION**

("Business Associate") entered into that certain Business Associate Agreement (the "Agreement") with Centene Corporation ("Centene"). Business Associate submits this attestation to Centene based on Business Associate's best knowledge, information and belief after having made a diligent inquiry.

1. For the period commencing from the later of (i) the Agreement's effective date or (ii) the date of the last Annual Attestation through the execution date of this Attestation set forth below, Business Associate has:
  - a. Promptly notified Centene in writing of all Incidents involving it, its affiliates and Subcontractors involving the PHI of any individual Business Associate and its affiliates have Used in connection with a Services Agreement.
  - b. Adhered to the privacy and security standards and requirements contained in the Agreement.
  - c. Incorporated into the contractual arrangement with any Subcontractor that Uses PHI the provisions required by the Agreement including executing a Business Associate Agreement between Business Associate and its business associate(s).
2. Business Associate has a documented security and privacy compliance program that complies with the requirements of (i) the HIPAA Authorities, (ii) applicable state security and privacy requirements, and (iii) all additional standards and obligations established by Centene pursuant to the Agreement and the Services Agreement(s).
3. Capitalized terms in this Attestation shall have the meaning ascribed to them in the Agreement unless defined otherwise herein.

[Name of Business Associate]

*E. Wolfe*  
Signature of Officer

Chair, Kitsap County  
Title of Signing Officer

Edward E. Wolfe  
Printed Name of Signing Officer

8-12-19  
Date

A signature below indicates that Business Associate no longer conducts the activities outlined in the Services Agreement(s) that require the Use of PHI and, consistent with state and federal law, has properly destroyed or returned to Coordinated Care Corp of WA all PHI in accordance with the Services Agreement(s) and the Agreement.

\_\_\_\_\_  
Signature of Officer

\_\_\_\_\_  
Title of Signing Officer

\_\_\_\_\_  
Printed Name of Signing Officer

\_\_\_\_\_  
Date

## **EXHIBIT 1 to ATTACHMENT D**

### **Delegated Provider Contracting**

In addition to the more general obligations of the parties set forth in the Agreement and Attachment D, this Exhibit 1 to Attachment D sets forth each Party's obligations specifically related to Delegated Provider Contracting Services.

BH-ASO contracts with BH-ASO Providers to provide certain behavioral health services to eligible individuals. Plan directly contracts with providers to provide health care, including behavioral health, services to its Members. Plan both conducts and delegates to BH-ASO responsibility for review and pricing of Provider Contracts, a Delegated Administrative Service ("Delegated Provider Contracting Services"). Plan has determined that BH-ASO is capable of assuming responsibility for performing Delegated Provider Contracting Services in accordance with the requirements of the Agreement.

1. **BH-ASO Obligations.** BH-ASO shall:

1.1. **Written Provider Contracts.** Enter into written contracts with BH-ASO Providers to provide Behavioral Health services to Plan Members as set forth in the Agreement.

1.1.1. Ensure that BH-ASO's Provider agreement forms shall comply with applicable Compliance Requirements.

1.2. **OIC Filing.** BH-ASO shall provide to Plan copies of its currently-in-use Provider Contract templates, including applicable amendment templates, for filing with the Washington State Office of the Insurance Commissioner as required when an issuer (Plan) utilizes a rented or leased network to provide health care services to its Members. BH-ASO shall provide Plan with new templates and/or amendment forms when such templates are updated.

1.3. **Provider Contracts – Contents.** Assure that BH-ASO's Provider Contracts with individual BH-ASO Providers:

1.3.1. Specify that Providers shall cooperate with BH-ASO's Quality Improvement program and shall maintain a quality improvement system tailored to the nature and type of health care services rendered under the Provider Contract, and which affords quality control for the health care provided.

1.3.2. Encourage open communication and cooperation with quality improvement activities.

1.3.3. Specify that Plan and BH-ASO have access to Providers medical records, to the extent permitted by state and federal law.

1.3.4. Specify that Providers must maintain the confidentiality of Member information and records.

1.3.5. Include an affirmative statement that Providers should freely communicate with Members about treatment options in Attachment B, including medication treatment options, regardless of benefit coverage limitations.

1.4. Provider Manual. BH-ASO shall maintain a Provider Manual, which BH-ASO shall provide to Plan for review and approve annually.

1.4.1. BH-ASO's Provider Manual shall contain information useful and applicable to Providers including policies and procedures and documents referring to credentialing, utilization management, prior authorization requirements, claims, submission, and online Provider demographic information.

1.5. BH-ASO shall be responsible for resolving all Provider complaints and appeals related to payment and other terms of BH-ASO's Provider Contracts.

2. Obligations of Plan. Plan shall:

2.1. Provide ongoing monitoring and periodic formal review of BH-ASO's performance hereunder that is consistent with industry standards, accreditations requirements, Plan's state and federal contracts and applicable state and federal laws and regulations, including those promulgated by the OIC.

2.2. Participate with the BH-ASO and BH-ASO subcontractors in crisis system enhancement planning, development, and monitoring. These activities will include mutual monitoring of crisis utilization.

2.3. Plan agrees to facilitate health care engagement for persons identified by Crisis system as needing emergent of urgent medical treatment.



## **ATTACHMENT E**

### **REPORTS**

**BH-ASO shall provide to the Plan the following data for crisis reporting on a monthly basis:**

- 1. The number of Plan Members served by the crisis system.**
- 2. The number and percentage of Plan Members referred for mobile outreach regardless of referral point (i.e., source of referral to the crisis line).**
- 3. The estimated percentage of calls to the crisis hotline success diverted from Emergency Rooms and/or ITA commitments.**
- 4. BH-ASO and Plan will collaborate to reach mutual agreement on the content and format of daily reporting.**

## **Coordinated Care Claims and Encounters Delegation Grid**

The purpose of the following grid is to specify the responsibilities of Salish Behavioral Health Administrative Services Organization (“Delegate”) under the Administrative Services Agreement with respect to the specific activities that are delegated regarding Claims and Encounter Data. The grid also describes the reporting requirements, which are in addition to any applicable reporting requirements stated in the Agreement. The grid below applies to the delegation of Claims Processing and Payment and Encounter Data Submission by MCO to Delegate.

The delegation grid may be amended from time to time during the term of the Agreement by MCO to reflect changes in delegation standards; delegation status; performance measures; reporting requirements; and other provisions.

The sections that follow describe the process by which MCO evaluates Delegate’s performance and the remedies available to MCO if Delegate does not fulfill its obligations. The statements below shall not supersede any term or condition of Exhibit A, the Delegation Agreement, and all obligations and remedies set forth in the parties’ Agreement remain in full force and effect. In the event of a conflict between the descriptions below and any term or condition of the Agreement, including Exhibit A, the terms and conditions of the Agreement shall prevail.

### **Process of Evaluating Delegate’s Performance**

MCO will require routine reports and documentation as listed in the delegation grid and will use this documentation to evaluate Delegate performance on an ongoing basis. In addition, MCO will:

- Conduct an annual audit to ensure all delegated activities comply with applicable Compliance Requirements,
- Provide written feedback on the results of the annual audit, and
- Require Delegate to implement corrective action plans if the delegate does not fully meet Compliance Requirements.

If MCO determines that Delegate has failed to adequately perform the delegated activities, MCO may:

- Change or revoke the scope of delegation if corrective action is not adequate; and/or
- Discontinue contracting with Delegate.

Ongoing performance of accredited delegates is evaluated through the semi-annual and routine monitoring of reports. MCO reserves the right to conduct annual and ad hoc audits of documentation, processes and files in order to ensure service levels, quality and compliance with regulatory requirements.

### **Corrective Action Plans**

If Delegate fails to meet any of its responsibilities, including contracted responsibilities and NCQA accreditation or certification standards, MCO will work with Delegate to create a

corrective action plan to identify areas of improvement and actions plans to ensure compliance with all elements and categories. If Delegate does not take corrective action, or fails to meet improvement goals, MCO reserves the right to revise the delegation agreement and scope, or revoke the delegation agreement altogether.

**Subdelegation**

It may be allowable for Delegate to subdelegate specific activities that relate to Claims and Encounter Data. As provided for under the Agreement and as set forth herein, subdelegation requires the prior written approval of MCO. In addition to the requirements for subdelegation set forth in the Agreement, Delegate will submit to MCO a Delegation Chart (template to be provided by MCO). If a subdelegation is approved, the Delegate will be responsible for ongoing oversight of the subdelegate’s performance and will be required to report performance results to MCO.

CLAIMS/ENCOUNTER BUSINESS REQUIREMENTS				
Function	Delegation	Delegation Authority	Reporting Frequency/ Submission	Cost
1. Encounter Data  Definition of Encounter Data	<input checked="" type="checkbox"/> Delegated  <input type="checkbox"/> Not Delegated	Encounter Data means records of physical or behavioral health care services submitted as electronic data files created by the Delegate’s system in the standard 837 format and the National Council for Prescription Drug Programs (NCPDP) Batch format.	N/A	N/A
2. Encounter Data  Dedicated Resource	<input checked="" type="checkbox"/> Delegated  <input type="checkbox"/> Not Delegated	Designate a person dedicated to work collaboratively with MCO on quality control and review of encounter data submitted to HCA.	N/A	MCO resource will partner with Delegate resource for quality control and review of encounter data.
3. Encounter Data		Submit complete,	Weekly	MCO will provide

Reporting requirements	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	accurate, and timely data for all services for which the Delegate has incurred any financial liability, whether directly or through subcontracts or other arrangements in compliance with current encounter submission guidelines as published by HCA.		oversight of Delegate encounter data.
4. Encounter Data Expected turnaround time reporting encounter data	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	Encounter data must be submitted to MCO at a minimum weekly, and no later than thirty (30) calendar days from the end of the month in which the Delegate paid the financial liability.	Weekly	MCO will monitor turnaround.
5. Encounter Data Submission and edits	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	Submitted encounters and encounter records must pass all system edits with a disposition of accept and listed in the Encounter Data Reporting Guide or sent out in communications from HCA to the Delegate.	N/A	N/A
6. Encounter Data Duplicates	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	Submitted encounters or encounter records must not be a duplicate of a previously submitted and accepted	N/A	N/A

		encounter or encounter record unless submitted as an adjustment or void per HIPAA Transaction Standards.		
7. Encounter Data RCW 42.56.270(11)	<input checked="" type="checkbox"/> Delegated  <input type="checkbox"/> Not Delegated	<p>The Delegate must report the paid date, paid unit, and paid amount for each encounter. The "paid amount" data is considered the Delegate's proprietary information and is protected from public disclosure.</p> <p>"Paid amount" is defined as the amount paid for the service, or zero pay for cost based/invoice payments.</p>	N/A	N/A
8. Encounter Data 42 C.F.R. § 438.606  Attestations	<input checked="" type="checkbox"/> Delegated  <input type="checkbox"/> Not Delegated	The Delegate shall send attestation to MCO to certify the accuracy and completeness of all encounter data concurrently with each file upload.	Weekly	MCO will receive monthly attestations from the Delegate. MCO will review and complete the monthly certification letter and send to the HCA.
9. Encounter Data 837 Requirements	<input checked="" type="checkbox"/> Delegated  <input type="checkbox"/> Not Delegated	THE Delegate must be able to meet the requirements outlined in the attached requirements document.	N/A	N/A
10. Encounter Data		The Delegate must	Quarterly	MCO will oversee

Quality Assurance	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	validate the accuracy and completeness of all encounter data for behavioral health care services compared to the year-to-date general ledger of paid claims for the health care services.		the quality assurance of the Delegate encounters.
11. Encounter Data  Form D	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	Within sixty (60) calendar days of the end of each calendar quarter, the Delegate shall provide aggregate totals of all encounter data submitted and accepted during that quarter on the Apple Health - Integrated Managed Care Quarterly Encounter/General Ledger Reconciliation (Form D). Delegate shall reconcile the cumulative encounter data submitted and accepted for the quarter and contract year with the general ledger paid claims for the quarter. The Delegate shall provide justification for any discrepancies.  Delegate will	Quarterly	MCO will submit Form D to HCA.

		<p>complete Form D and send to MCO.</p> <p>HCA will approve or reject the discrepancy justifications and notify the MCO of the decision 120 calendar days of the end of each calendar quarter.</p>		
<p><b>12. Claims Payment Standards</b></p> <p>Section 1902(a)(37) of the Social Security Act</p> <p>42 C.F.R. § 447.46</p> <p>WAC 284-170-431</p>	<p><input checked="" type="checkbox"/> Delegated</p> <p><input type="checkbox"/> Not Delegated</p>	<p>The Delegate shall meet the timeliness of payment standards. These standards shall also be applicable to State-only and federal block grant fund payments.</p> <p>To be compliant with payment standards the Delegate shall pay or deny 95 percent of clean claims within thirty (30) calendar days of receipt, 95 percent of all claims within sixty (60) calendar days of receipt and 95 percent of clean claims within ninety (90) calendar days of receipt.</p> <p>The Delegate shall provide a monthly report to the MCO of claims timeliness results. If standard is not met, provide</p>	Monthly	MCO will monitor timeliness of claims payment standards.

		root cause and corrective action until performance expectation is met.		
<p>13. Claims processing</p> <p>Top Claims Denials Reporting</p>	<p><input checked="" type="checkbox"/> Delegated</p> <p><input type="checkbox"/> Not Delegated</p>	<p>The Delegate shall produce and submit a quarterly claims denial analysis report. The first report due May 31<sup>st</sup> 2019 for services processed January – March 2019. The report shall include the following data:</p> <p>Total number of approved claims for which there was at least one denied line.</p> <p>Completely denied claims.</p> <p>Total number of claims adjudicated in the reporting claim.</p> <p>Total number of behavioral health claims denied by claim line.</p> <p>Summary by reason and type of claims denied.</p> <p>The total number of denied claims divided by the total number of claims.</p> <p>For each of the five network billing providers with the</p>	Quarterly	MCO will review denials, and may report up to the HCA.



		<p>highest number of total denied claims, the number of total denied claims expressed as a ratio to all claims adjudicated.</p> <p>Total number of Behavioral Health claims received, that were not approved upon initial submission.</p> <p>The total number of rejected/non-clean behavioral health claims, divided by the total number of claims submitted.</p> <p>The top five reasons for behavioral health claims being rejected upon initial submission.</p> <p>The report shall include a narrative, including the action steps planned to address.</p> <p>The top five (5) reasons for denial, including provider education to the five network billing providers with the highest number of total denied claims. Provider education must address root causes of denied claims and actions</p>		
--	--	---	--	--

		to address them.		
14. TPL Reporting	<input checked="" type="checkbox"/> Delegated  <input type="checkbox"/> Not Delegated	<p>The Delegate shall submit a quarterly <i>Recovery and Cost Avoidance Report</i> that includes any recoveries for third party resources as well as claims that the Delegate denies due to TPL coverage. The report shall include recoveries or denied claim payments for any covered service. The Delegate shall calculate cost savings in categories. The Delegate shall treat funds recovered from third parties as offsets to claims payments and reflect those offsets in encounter data. The report is due by the sixtieth (60th) calendar day following the end of the quarter.</p> <p>The Delegate shall submit to the MCO on the 15th of the month</p>	Monthly	MCO will review and report outcome to the HCA.

		<p>following the end of the monthly reporting period a report (Enrollees with Other Health Care Insurance) of Enrollees with any other health care insurance coverage with any carrier, including the Delegate.</p> <p>The Delegate shall submit to the MCO on the 20th of the following month a report (Subrogation Rights of Third Party Liability (TPL) – Investigations) of any Enrollees who the Delegate newly becomes aware of a cause of action to recover health care costs for which the Delegate has paid under the Agreement.</p>		
15. Participating and Non-Participating Reporting	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	The Delegate shall track and record all payments to Participating Providers and Non-Participating Providers in a manner that		MCO will monitor, and may report up to the HCA.

		<p>allows for reporting to the MCO the number, amount, and percentage of claims paid to Participating Providers and Non-Participating Providers separately. The Delegate shall identify the type of providers and Subspecialty. The Delegate shall also track, document and report to the MCO any known attempt by Non-Participating Providers to balance bill Enrollees.</p> <p>The Delegate shall provide annual reports to the MCO for the preceding state fiscal year (July 1 through June 30). The reports shall indicate the proportion of services provided by the Delegate's Participating Providers and Non-Participating Providers, by county, and including</p>		
--	--	--	--	--

		hospital-based physician services. Delegate shall submit the reports to the MCO no later than August 15 of each year.		
16. Sub-delegation Agreements  Delegate sub-delegation agreements with a vendor	<input type="checkbox"/> Delegated  <input checked="" type="checkbox"/> Not Delegated	Notify the MCO of sub-delegation vendor agreements the Delegate has; what duties do they perform, and how often.		N/A
17. Claims/Encounter Delegation Oversight Audit  Quality Assurance Audits	<input type="checkbox"/> Delegated  <input checked="" type="checkbox"/> Not Delegated	<p>MCO is required to perform an annual oversight delegation audit of encounter data reporting/ claims processing.</p> <p>The objective of this audit is to assess the effectiveness of key internal controls by ensuring the accuracy, completeness, and timeliness of the encounter/claims processing functions.</p> <p>Delegate will provide MCO claims data set for specified time period.</p>	Annual	<p>MCO will review the claims data set for the following:</p> <ul style="list-style-type: none"> <li>• Review encounter/claims universe sample of all claims paid or denied for 1 year;</li> <li>• Verify the member was eligible for benefits on the dates of service;</li> <li>• Review encounter submission and reconciliation to ensure requirements are met;</li> <li>• Review claim payment calculations and verify that claims were paid accurately;</li> <li>• Verify claims were submitted by the provider within 365 days of dates of service;</li> <li>• Review responses to audit</li> </ul>

				questionnaire to ensure compliance.
--	--	--	--	-------------------------------------

**Coordinated Care of Washington**

Address: 1145 Broadway Ste 300  
Tacoma WA 98402

Phone: 877-644-4613

Email: Beth.Johnson@

coordinatedcarehealth.com

Signature

By: [Signature]

Title: President + CEO

Date: 8/15/19

**SALISH BEHAVIORAL HEALTH  
ADMINISTRATIVE SERVICES  
ORGANIZATION, BY KITSAP  
COUNTY BOARD OF  
COMMISSIONERS, Its Administrative  
Entity**

Address: 614 Division St. MS-23  
Port Orchard, WA 99366

Phone: 800-525-5637

Email: slew@sco.kitsap.wa.us

[Signature]

Edward E. Wolfe, Chair

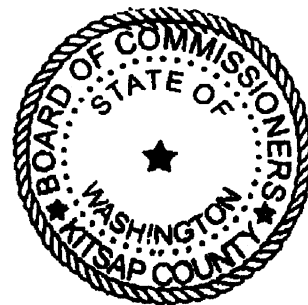
[Signature]  
Charlotte Garrido, Commissioner

[Signature]

Robert Gelder, Commissioner 9-12-19

ATTEST:

[Signature]  
Dana Daniels, Clerk of the Board



## **Coordinated Care Crisis Services – Additional Delegation Requirements Grid**

The purpose of this Crisis Services Delegation Grid is to specify the responsibilities of Salish Behavioral Health Administrative Services Organization (“Delegate”) under the Administrative Services Agreement] between Coordinated Care (“MCO”) and Delegate with respect to the specific activities that are delegated for Crisis Services, including reporting requirements.

“Crisis Services,” as defined by the HCA, means evaluation and treatment of mental health crisis to all Medicaid-enrolled individuals experiencing a crisis. A mental health crisis is defined as a turning point in the course of anything decisive or critical, a time, a stage, or an event or a time of great danger or trouble, whose outcome decides whether possible bad consequences will follow. Crisis Services shall be available on a 24-hour basis. Crisis Services are intended to stabilize the person in crisis, prevent further deterioration and provide immediate treatment and intervention in a location best suited to meet the needs of the individual and in the least restrictive environment available. Crisis Services may be provided prior to completion of an Intake Evaluation. Services are provided by or under the supervision of a Mental Health Professional.

The delegation grid may be amended from time to time during the term of this Agreement by MCO to reflect changes in delegation standards; delegation status; performance measures; reporting requirements; and other provisions.

The sections that follow describe the process by which MCO evaluates Delegate’s performance and the remedies available to MCO if Delegate does not fulfill its obligations.

### **Process of Evaluating Delegate’s Performance**

MCO will require routine reports and documentation as listed in the delegation grid and will use this documentation to evaluate Delegate performance on an ongoing basis. In addition MCO will:

- Conduct an annual audit to ensure all delegated activities comply with applicable delegation standards,
- Provide written feedback on the results of the annual audit, and
- Require Delegate to implement corrective action plans if the delegate does not fully meet delegation requirements.

If MCO determines that Delegate has failed to adequately perform the delegated activities, MCO may:

- Change or revoke the scope of delegation if corrective action is not adequate; and/or
- Discontinue contracting with Delegate.

Ongoing performance of accredited delegates is evaluated through the semi-annual and routine monitoring of reports. MCO reserves the right to conduct annual and ad hoc audits of

documentation, processes and files in order to ensure service levels, quality and compliance with regulatory requirements.

**Corrective Action Plans**

If Delegate fails to meet any of its responsibilities, including contracted responsibilities and NCQA accreditation or certification standards, MCO will work with Delegate to create a corrective action plan to identify areas of improvement and actions plans to ensure compliance with all elements and categories. If Delegate does not take corrective action, or fails to meet improvement goals, MCO reserves the right to revise the delegation agreement and scope, or revoke the delegation agreement all together.

**Subdelegation**

It may be allowable for Delegate to subdelegate specific activities that relate to Crisis Services. As provided for under the Agreement and as set forth herein, subdelegation requires the prior written approval of MCO. In addition to the requirements for subdelegation set forth in the Agreement, Delegate will submit to MCO a Delegation Chart (template to be provided by MCO). If a subdelegation is approved, the Delegate will be responsible for ongoing oversight of the subdelegate's performance and will be required to report performance results to MCO.

Function	Delegation Status	Delegate Activities	Reporting: Date, Frequency, & Submission	MCO Activities
<b>HCA CONTRACT REQUIREMENTS</b>				
24-7 Availability	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	Crisis Services shall be available 24-7-365, including regional crisis hotline that provides screening and referral services		
Immediate Access	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	Crisis Services shall be available to Members without the need for the member to complete an intake evaluation or other screening or assessment processes.		



Function	Delegation Status	Delegate Activities	Reporting Data, Frequency & Submission	MCO Activities
Encounter Data	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	Require submission of complete and accurate encounter data related to the provision of Crisis Services in HCA-prescribed formats	Weekly basis provide to MCO batches of such data	

Function	Delegation Status	Delegate Activities	Reporting Data, Frequency & Submission	MCO Activities
<b>WASHINGTON ADMINISTRATIVE CODE REQUIREMENTS</b>				
Crisis Services standards	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	Crisis services shall be performed in accordance with all state agency requirements, including Washington Department of Health and HCA regulatory requirements, applicable to Crisis Services and Crisis Services providers		

**Coordinated Care of Washington**

Address: 1145 Broadway Ste 300  
Tacoma, WA 98402

Phone: 877-644-4613

Email: beth.johnson@

coordinatedcarehealth.com  
Signature

By: [Signature]

Title: President & CEO

Date: 8/15/19

**SALISH BEHAVIORAL HEALTH  
ADMINISTRATIVE SERVICES  
ORGANIZATION, BY KITSAP  
COUNTY BOARD OF  
COMMISSIONERS, Its Administrative  
Entity**

Address: 614 Division St. MS-23  
Port Orchard, WA 98366

Phone: 800-525-5637

Email: sjlew@co.kitsap.wa.us

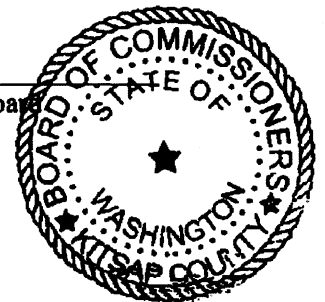
[Signature]  
Edward E. Wolfe, Chair

[Signature]  
Charlotte Garrido, Commissioner

[Signature]  
Robert Gelder, Commissioner 8-12-19

ATTEST:

[Signature]  
Dana Daniels, Clerk of the Board



## **Coordinated Care Crisis Services Delegation Grid**

The purpose of the following grid is to specify the responsibilities of Salish Behavioral Health Administrative Services Organization (“Delegate”) under the [Administrative Services Agreement] between Coordinated Care (“MCO” and Delegate with respect to the specific activities that are delegated for Crisis Services. The grid also describes at minimum semi-annual reporting requirements. The specific scope of activities that relates to this delegation arrangement includes Behavioral Health Crisis Services. These activities may not be sub-delegated without notification to, and prior approval by, MCO. (See section below on subdelegation.)

The delegation grid may be amended from time to time during the term of this Agreement by MCO to reflect changes in delegation standards; delegation status; performance measures; reporting requirements; and other provisions.

The process by which MCO evaluates Delegate performance and the remedies available to MCO if Delegate does not fulfill its obligations are as follows.

### **Process of Evaluating Delegate’s Performance**

MCO will require routine reports and documentation as listed in the delegation grid and will use this documentation to evaluate Delegate performance on an ongoing basis. In addition MCO will:

- Conduct an annual audit, to be performed offsite or onsite, to ensure compliance with all delegated activities,
- Provide written feedback on the results of the annual audit, and
- Implement corrective action plans if the delegate does not fully meet delegation requirements.

The consequences for failure to perform can include:

- Change or revoke the scope of delegation if corrective action is not adequate; and/or
- Discontinue contracting with Delegate

On-going performance of accredited delegates is evaluated through the semi-annual and routine monitoring of reports. MCO reserves the right to conduct annual or ad hoc audits of documentation, processes and files in order to ensure service levels, quality and compliance with regulators.

### **Corrective Action Plans**

If Delegate fails to meet any of its responsibilities, including contracted responsibilities and NCQA accreditation or certification requirements, MCO will work with Delegate to create a corrective action plan to identify areas of improvement and actions plans to ensure compliance

with all elements and categories. If Delegate does not take corrective action, or fails to meet improvement goals, MCO reserves the right to revise the delegation agreement and scope, or revoke the delegation agreement all together.

**Subdelegation**

It may be allowable for a Delegate to subdelegate specific activities that relate to Crisis Services. Subdelegation will require prior written approval by MCO. In addition to the requirements for subdelegation set forth in the Agreement, Delegate will submit to MCO a Delegation Chart (template to be provided by MCO). If the Delegate chooses to subdelegate any activities, the Delegate is giving the sub-delegate authority to perform the delegated activities. As such, the Delegate is responsible for ongoing oversight of the subdelegate's performance and is required to report performance results to MCO.

**CRISIS SERVICES DELEGATION GRID**

Function	Delegation Status	Delegation Authority	Reporting Data, Frequency, & Submission	MCO Approval
<p>388-877-0900 Crisis mental health (MH) services—General</p>	<p><input checked="" type="checkbox"/> Delegated</p> <p><input type="checkbox"/> Not Delegated</p>	<p><u>Agency staff requirements:</u></p> <p>1) All crisis mental health services are provided by, or under the supervision of, a mental health professional;</p> <p>2) Each staff member working directly with an individual receiving any crisis mental health service in WAC 388-877-0905 through 388-877-0920 receives:</p> <p style="padding-left: 20px;">a) Clinical supervision from a mental health professional and/or an independent practitioner licensed by department of health; and</p> <p style="padding-left: 20px;">b) Annual violence prevention training on the safety and violence prevention topics described in RCW 49.19.030. The staff member's personnel record must document the training.</p>	<p>Deliver the following in electronic format to MCO 12 months following the execution of the delegation agreement, and annually thereafter:</p> <p>Applicable policies and procedures for agency staff requirements and record content and documentation requirements.</p> <p>Evidence of current qualifications of MHPs and clinical supervisors.</p> <p>Documentation of violence prevention training.</p> <p>List of current professional consultants.</p> <p>Documentation audit process and results of annual documentation audits for</p>	<p>MCO will receive and review the policies and procedures, protocols, documentation and reports.</p>

		<p>3) Staff access to consultation with one of the following professionals who has at least one year's experience in the direct treatment of individuals who have a mental or emotional disorder:</p> <ul style="list-style-type: none"> <li>a) A psychiatrist;</li> <li>b) A physician;</li> </ul> <p>or</p> <ul style="list-style-type: none"> <li>c) An advanced registered nurse practitioner (ARNP) who has prescriptive authority.</li> </ul> <p><u>Record content and documentation requirements:</u>  An agency providing any crisis mental health service in WAC 388-877-0905 through 388-877-0920 and 388-877-0810 must maintain a record that contains timely documentation. Documentation must include the following, as applicable to the crisis service provided:</p> <ul style="list-style-type: none"> <li>1) A brief summary of each crisis service encounter, including the date,</li> </ul>	<p>compliance with record content and documentation requirements, and documentation of any corrective actions taken on identified opportunities for improvement.</p>	
--	--	--	--	--

		<b>time, and duration of the encounter; 2) The names of the participants; and 3) A follow-up plan, including any referrals for services, including emergency medical services.</b>		
--	--	--	--	--

<p>388-877-0905 Crisis mental health services— Telephone support services</p>	<p><input checked="" type="checkbox"/> Delegated  <input type="checkbox"/> Not Delegated</p>	<p>Mental health telephone support services are services provided as a means of first contact to an individual in crisis. These services may include deescalation and referral.</p> <p>1) The agency must:</p> <ul style="list-style-type: none"> <li>a) Respond to crisis calls twenty-four-hours-a-day, seven-days-a week;</li> <li>b) Have a written protocol for the referral of an individual to a voluntary or involuntary treatment facility for admission on a seven-day-a-week, twenty-four-hour-a-day basis, including arrangements for contacting the designated crisis responder</li> <li>c) Assure communication and coordination with the individual's mental health care provider, if indicated and appropriate;</li> <li>d) Post a copy of the statement of individual</li> </ul>	<p>Deliver the following in electronic format to MCO 12 months following the execution of the delegation agreement, and annually thereafter:</p> <p>Applicable policies and procedures and protocols.</p> <p>Monthly Summary Call logs</p>	<p>MCO will receive and review the policies and procedures, protocols, documentation and reports including monthly summary call logs.</p>
---	--	---	--	---



		<p>rights in a location visible to staff and agency volunteers.</p> <p>2) An agency must document each telephone crisis response contact made. (includes subsections a-d)</p>		
<p>388-877-0910 Crisis mental health services— Outreach services</p>	<p><input checked="" type="checkbox"/> Delegated</p> <p><input type="checkbox"/> Not Delegated</p>	<p>Crisis outreach services are face-to-face intervention services provided to assist individuals in a community setting. A community setting can be an individual's home, an emergency room, a nursing facility, or other private or public location. An agency providing crisis outreach services must:</p> <p>1) Provide crisis telephone screening. 2) Have staff available twenty-four hours a day, seven days a week to respond to a crisis. 3) Ensure face-to-face outreach services are provided by a mental health professional, or a staff member under the supervision of a mental health professional with documented training in crisis response. 4) Ensure services are provided in a setting</p>	<p>Deliver the following in electronic format to MCO 12 months following the execution of the delegation agreement, and annually thereafter:</p> <p>Applicable policies and procedures for crisis outreach services.</p> <p>Results of delegate's most recent annual audit of outreach services for compliance with WAC 388-877-0910, and report on any corrective actions taken on identified opportunities for improvement.</p>	<p>MCO will receive and review the policies and procedures, protocols, documentation and reports.</p>

		<p>that provides for the safety of the individual and agency staff members.</p> <p>5) Have a protocol for requesting a copy of an individual's crisis plan twenty-four hours a day, seven days a week.</p> <p>6) Require that staff member(s) remain with the individual in crisis in order to provide stabilization and support until the crisis is resolved or a referral to another service is accomplished.</p> <p>7) Resolve the crisis in the least restrictive manner possible.</p> <p>8) Have a written plan for training, staff back-up, information sharing, and communication for staff members who respond to a crisis in an individual's private home or in a nonpublic setting.</p> <p>9) Ensure that a staff member responding to a crisis is able to be accompanied by a second trained individual when services are provided in the individual's home or other nonpublic location.</p> <p>10) Ensure that any staff member who engages in home</p>		
--	--	---	--	--

		<p>visits is provided by their employer with a wireless telephone, or comparable device for the purpose of emergency communication as described in RCW 71.05.710.</p> <p>11) Provide staff members who are sent to a private home or other private location to evaluate an individual in crisis, prompt access to information about any history of dangerousness or potential dangerousness on the individual they are being sent to evaluate that is documented in a crisis plan(s) or commitment record(s). This information must be made available without unduly delaying the crisis response.</p> <p>12) Have a written protocol that allows for the referral of an individual to a voluntary or involuntary treatment facility twenty-four hours a day, seven days a week.</p> <p>13) Have a written protocol for the transportation of an individual in a safe</p>		
--	--	---	--	--

		<p>and timely manner, when necessary.</p> <p>14) Document all crisis response contacts, including:</p> <ul style="list-style-type: none"> <li>a) The date, time, and location of the initial contact.</li> <li>b) The source of referral or identity of caller.</li> <li>c) The nature of the crisis.</li> <li>d) Whether the individual has a crisis plan and any attempts to obtain a copy.</li> <li>e) The time elapsed from the initial contact to the face-to-face response.</li> <li>f) The outcome, including: <ul style="list-style-type: none"> <li>i) The basis for a decision not to respond in person;</li> <li>ii) Any follow-up contacts made; and</li> <li>iii) Any referrals made, including referrals to emergency medical services.</li> </ul> </li> <li>g) The name of the staff person(s) who responded to the crisis.</li> </ul>		
<p>388-877-0915 Crisis mental health services— Stabilization services</p>	<p><input checked="" type="checkbox"/> Delegated</p> <p><input type="checkbox"/> Not Delegated</p>	<p>Crisis mental health stabilization services include short-term (less than two weeks per episode) face-to-face assistance with life skills training and understanding of medication effects on</p>	<p>Deliver the following in electronic format to MCO 12 months following the execution of the delegation agreement, and</p>	<p>MCO will receive and review the policies and procedures, protocols, documentation and reports.</p>

		<p>an individual. Stabilization services may be provided to an individual as a follow-up to crisis services provided or to any individual determined by a mental health professional to need additional stabilization services. In addition to meeting the general requirements for crisis services in WAC <u>388-877-0900</u>, an agency certified to provide crisis stabilization services must</p> <p>(1) Ensure the services are provided by a mental health professional, or under the supervision of a mental health professional;</p> <p>(2) Ensure the services are provided in a setting that provides for the safety of the individual and agency staff;</p> <p>(3) Have a written plan for training, staff back-up, information sharing, and communication for staff members who are providing stabilization services in an individual's private home or in a nonpublic setting;</p> <p>(4) Have a protocol for requesting a copy of</p>	<p>annually thereafter:</p> <p>Applicable policies and procedures and protocols.</p>	
--	--	---	--	--

		<p>an individual's crisis plan;</p> <p>(5) Ensure that a staff member responding to a crisis is able to be accompanied by a second trained individual when services are provided in the individual's home or other nonpublic location;</p> <p>(6) Ensure that any staff member who engages in home visits is provided by their employer with a wireless telephone, or comparable device, for the purpose of emergency communication as described in RCW <u>71.05.710</u>;</p> <p>(7) Have a written protocol that allows for the referral of an individual to a voluntary or involuntary treatment facility;</p> <p>(8) Have a written protocol for the transportation of an individual in a safe and timely manner, when necessary; and</p> <p>(9) Document all crisis stabilization response contacts, including identification of the staff person(s) who responded.</p>		
--	--	---	--	--

<p>388-877-0920 Crisis mental health services— Peer support</p>	<p><input checked="" type="checkbox"/> Delegated  <input type="checkbox"/> Not Delegated</p>	<p>Crisis peer support services assist an individual in exercising control over their own life and recovery process through the practice of peer counselors sharing their own life experiences related to mental illness to build alliances that enhance the individual's ability to function.</p> <p>1) Peer support services are intended to augment and not supplant other necessary mental health services.</p> <p>2) An agency providing crisis peer support services must:</p> <p style="padding-left: 20px;">a) Ensure services are provided by a person recognized by the division of behavioral health and recovery (DBHR) as a peer counselor, as defined in WAC 388-877-0900, under the supervision of a mental health professional.</p> <p style="padding-left: 20px;">b) Ensure services provided by a peer counselor are within the scope of the peer counselor's training and credential.</p> <p style="padding-left: 20px;">c) Ensure that a peer counselor</p>	<p>Deliver the following in electronic format to MCO 12 months following the execution of the delegation agreement, and annually thereafter:</p> <p>Applicable policies and procedures for peer support services.</p> <p>Results of delegate's most recent annual audit of crisis peer support services for compliance with WAC 388-877-0920, and report on any corrective actions taken on identified opportunities for improvement.</p>	<p>MCO will receive and review the policies and procedures, protocols, documentation and reports.</p>
---	--	---	---	---

		<p>responding to a crisis is accompanied by a mental health professional.</p> <p>d) Ensure that any staff member who engages in home visits is provided by their employer with a wireless telephone, or comparable device, for the purpose of emergency communication.</p> <p>e) Ensure peer counselors receive annual training that is relevant to their unique working environment.</p>		
--	--	---	--	--



<p>388-877-0810  Involuntary and court ordered—  Emergency involuntary  detention mental  health and  substance use  disorder services</p>	<p><input checked="" type="checkbox"/> Delegated   <input type="checkbox"/> Not  Delegated</p>	<p>Emergency involuntary detention services are services provided by a designated crisis responder (DCR) to evaluate an individual in crisis and determine if involuntary services are required. In addition to meeting the behavioral health agency licensure, certification, administration, personnel, and clinical requirements in WAC <u>388-877-0300</u> through <u>388-877-0680</u>, an agency certified to provide emergency involuntary detention services must do all of the following:</p> <p>(1) Ensure that services are provided by a DCR.</p> <p>(2) Ensure staff members are available twenty-four hours a day, seven days a week.</p> <p>(3) Ensure staff members utilize the protocols for DCRs required by RCW <u>71.05.214</u>.</p> <p>(4) Have a written agreement with a certified inpatient evaluation and treatment or secure withdrawal management and</p>	<p>Deliver the following in electronic format to MCO 12 months following the execution of the delegation agreement, and annually thereafter:</p> <p>Applicable policies and procedures and protocols.</p>	<p>MCO will receive and review the policies and procedures, protocols, documentation and reports.</p>
--	--	---	---	---

		<p>stabilization facility to allow admission of an individual twenty-four hours a day, seven days a week.</p> <p>(5) Have a plan for training, staff back-up, information sharing, and communication for a staff member who responds to a crisis in a private home or a nonpublic setting.</p> <p>(6) Ensure that a DCR is able to be accompanied by a second trained individual when responding to a crisis in a private home or a nonpublic setting.</p> <p>(7) Ensure that a DCR who engages in a home visit to a private home or a nonpublic setting is provided by their employer with a wireless telephone, or comparable device, for the purpose of emergency communication as described in RCW <u>71.05.710</u>.</p> <p>(8) Provide staff members, who are sent to a private home or other private location to evaluate an individual in crisis, prompt access to information about any history of dangerousness or</p>		
--	--	---	--	--

		<p>potential dangerousness on the individual they are being sent to evaluate that is documented in a crisis plan(s) or commitment record(s). This information must be made available without unduly delaying the crisis response.</p> <p>(9) Have a written protocol for the transportation of an individual, in a safe and timely manner, for the purpose of medical evaluation or detention.</p> <p>(10) Document services provided to the individual, and other applicable information. At a minimum this must include:</p> <p>(a) That the individual was advised of their rights in accordance with RCW <u>71.05.360</u>;</p> <p>(b) That if the evaluation was conducted in a hospital emergency department or inpatient unit, it occurred in accordance with the timelines required by RCW <u>71.05.050</u>.</p>		
--	--	---	--	--

		<p><u>71.05.153</u>, and <u>71.34.710</u>;</p> <p>(c) That the DCR conducting the evaluation considered both of the following when evaluating the individual:</p> <p>(i) The imminent likelihood of serious harm or imminent danger because of being gravely disabled (see RCW <u>71.05.153</u>); and</p> <p>(ii) The likelihood of serious harm or grave disability that does not meet the imminent standard for the emergency detention (see RCW <u>71.05.150</u>);</p> <p>(d) That the DCR documented consultation with any examining emergency room physician as required by RCW <u>71.05.154</u>;</p> <p>(e) If the individual was not detained:</p> <p>(i) A description of the disposition and follow-up plan; and</p> <p>(ii) Documentation that the minor's parent was informed of their right to request a court review of the DCR's decision not to</p>		
--	--	--	--	--

		<p>detain the minor under RCW <u>71.34.710</u>, if the individual is a minor thirteen years of age or older;</p> <p>(f) If the individual was detained, a petition for initial detention must include the following:</p> <p>(i) The circumstances under which the person's condition was made known;</p> <p>(ii) Evidence, as a result of the DCR's personal observation or investigation, that the actions of the person for which application is made constitute a likelihood of serious harm, or that the individual is gravely disabled;</p> <p>(iii) Evidence that the individual will not voluntarily seek appropriate treatment;</p> <p>(iv) Consideration of all reasonably available information from credible witnesses, to include family members, landlords, neighbors, or others with significant contact and history of involvement with the individual, and</p>		
--	--	--	--	--

		<p>records, as required by RCW <u>71.05.212</u>; and</p> <p>(v)  Consideration of the individual's history of judicially required, or administratively ordered, anti-psychotic medications while in confinement when conducting an evaluation of an offender under RCW <u>72.09.370</u>; and</p> <p>(g)  Documentation that the individual, or the individual's guardian or conservator, received a copy of the following:</p> <ul style="list-style-type: none"> <li>(i) Notice of detention;</li> <li>(ii) Notice of rights; and</li> <li>(iii) Initial petition.</li> </ul>		
--	--	--	--	--

**Coordinated Care of Washington**

Address: 1145 Broadway Ste 300  
Tacoma, WA 98402

Phone: 877-644-4613

Email: Beth.Johnson@

Coordinatedcarehealth.com  
Signature

By: [Signature]

Title: President & CEO

Date: 8/15/19

**SALISH BEHAVIORAL HEALTH  
ADMINISTRATIVE SERVICES  
ORGANIZATION, BY KITSAP  
COUNTY BOARD OF  
COMMISSIONERS, Its Administrative  
Entity**

Address: 614 Division St, MS-23  
Port Orchard, WA 98366

Phone: 800-525-5637

Email: gilewis@co.kitsap.wa.us

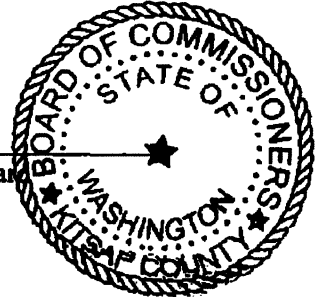
[Signature]  
Edward E. Wolfe, Chair

[Signature]  
Charlotte Garrido, Commissioner

[Signature] 9-12-19  
Robert Gelder, Commissioner

ATTEST:

[Signature]  
Dana Daniels, Clerk of the Board



## **Coordinated Care Quality Improvement (QI) Delegation Grid**

The purpose of the following grid is to specify the responsibilities of Salish Behavioral Health Administrative Services Organization (“Delegate”) under the [Administrative Services Agreement] between Coordinated Care (“MCO”) and Delegate with respect to the specific activities that are delegated for behavioral health Quality Improvement. The grid also describes at minimum semi-annual reporting requirements. The specific scope of activities that relates to this delegation arrangement includes Behavioral Health Telephone Access for Crisis Services. These activities may not be sub-delegated without notification to, and prior approval by, MCO. (See section below on subdelegation.)

MCO does not broadly delegate the responsibility for performing quality management and improvement activities on behalf of MCO. However, MCO does require Delegates to maintain a quality improvement and management program pertaining to delegated activities, and participate and cooperate in MCO quality improvement program, collect data for MCO quality improvement activities, and carry out corrective actions as required by MCO.

The delegation grid may be amended from time to time during the term of this Agreement by MCO to reflect changes in delegation standards; delegation status; performance measures; reporting requirements; and other provisions.

The process by which MCO evaluates Delegate performance and the remedies available to MCO if Delegate does not fulfill its obligations are as follows.

### **Process of Evaluating Delegate’s Performance**

MCO will require routine reports and documentation as listed in the delegation grid and will use this documentation to evaluate Delegate performance on an ongoing basis. In addition MCO will:

- Conduct an annual audit, to be performed offsite or onsite, to ensure compliance with all delegated activities,
- Provide written feedback on the results of the annual audit, and
- Implement corrective action plans if the delegate does not fully meet delegation requirements.

The consequences for failure to perform can include:

- Change or revoke the scope of delegation if corrective action is not adequate; and/or
- Discontinue contracting with Delegate

On-going performance of accredited delegates is evaluated through the semi-annual and routine monitoring of reports. MCO reserves the right to conduct annual or ad hoc audits of documentation, processes and files in order to ensure service levels, quality and compliance with regulators.



**Corrective Action Plans**

If Delegate fails to meet any of its responsibilities, including contracted responsibilities and NCQA accreditation or certification requirements, MCO will work with Delegate to create a corrective action plan to identify areas of improvement and actions plans to ensure compliance with all elements and categories. If Delegate does not take corrective action, or fails to meet improvement goals, MCO reserves the right to revise the delegation agreement and scope, or revoke the delegation agreement all together.

**Subdelegation**

It may be allowable for a Delegate to subdelegate specific activities that relate to Crisis Services telephone operations. Subdelegation will require prior written approval by MCO. In addition to the requirements for subdelegation set forth in the Agreement, Delegate will submit to MCO a Delegation Chart(template to be provided by MCO). If the Delegate chooses to subdelegate any activities, the Delegate is giving the sub-delegate authority to perform the delegated activities. As such, the Delegate is responsible for ongoing oversight of the subdelegate’s performance and is required to report performance results to MCO.

DELEGATION GRID				
Function	Delegation Status	Delegate Activities	Reporting Data Frequency & Submission	MCO Activities
Behavioral Health Telephone Access [QI 4.B.1 and QI 4.B.2]	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	Telephones are answered by a live voice within 30 seconds with an abandonment rate within 5 percent.	Submission to MCO staff of a quarterly summary report that includes total calls, call answer time and abandonment rate. Reports provided in electronic or hard copy.	MCO staff will receive and review quarterly reports for performance review.

**Coordinated Care of Washington**

Address: 1145 Broadway Ste 200  
Tacoma, WA 98402

Phone: 877-644-4113

Email: Beth.Johnson@

CoordinatedCareHealth.com  
Signature

By: [Signature]

Title: President + CEO

Date: 8/15/19

**SALISH BEHAVIORAL HEALTH  
ADMINISTRATIVE SERVICES  
ORGANIZATION, BY KITSAP  
COUNTY BOARD OF  
COMMISSIONERS, Its Administrative  
Entity**

Address: 614 Division St, MS-23  
Port Orchard, WA 98366

Phone: 800-625-5637

Email: Silewis@Co.Kitsap.wa.us

[Signature]  
Edward E. Wolfe, Chair

[Signature]  
Charlotte Garrido, Commissioner

[Signature]  
Robert Gelder, Commissioner

8-12-19

ATTEST:

[Signature]  
Dana Daniels, Clerk of the Board

## **Coordinated Care Credentialing and Recredentialing Delegation Grid**

The purpose of the following grid is to specify the responsibilities of Salish Behavioral Health Administrative Services Organization (“Delegate”) under the [Administrative Services Agreement] between MCO and Delegate with respect to the specific activities that are delegated for credentialing and recredentialing of certain behavioral health providers. The grid also describes the semi-annual reporting requirements. The specific scope of activities that relates to this delegation arrangement includes: credentialing and recredentialing of certain behavioral health providers that are contracted directly with Delegate. These activities may not be sub-delegated without notification to, and prior approval by, MCO. (See section below on subdelegation.)

The delegation grid may be amended from time to time during the term of this Agreement by MCO to reflect changes in delegation standards; delegation status; performance measures; reporting requirements; and other provisions.

MCO will provide member experience and clinical performance data as requested by the Delegate and if it is relevant to the delegated responsibilities or activities. Member experience data may include: complaints, CAHPS 5.0H Survey results or other data collected on members’ experience with the delegate’s services. Clinical performance data may include: HEDIS measures, claims and other clinical data collected by the organization.

The process by which MCO evaluates Delegate performance and the remedies available to MCO if Delegate does not fulfill its obligations are as follows.

### **Process of Evaluating Delegate’s Performance**

[MCO will require routine reports and documentation as listed in the delegation grid and will use this documentation to evaluate Delegate performance on an ongoing basis. In addition [MCO will:

- Conduct an annual audit, to be performed offsite or onsite, to ensure compliance with all delegated activities,
- Provide written feedback on the results of the annual audit, and
- Implement corrective action plans if the delegate does not fully meet delegation requirements.

The consequences for failure to perform can include:

- Change or revoke the scope of delegation if corrective action is not adequate; and/or
- Discontinue contracting with Delegate

On-going performance of accredited delegates is evaluated through the semi-annual and routine monitoring of reports. [MCO reserves the right to conduct annual or ad hoc audits of documentation, processes and files in order to ensure service levels, quality and compliance with regulators.

**Corrective Action Plans**

If Delegate fails to meet any of its responsibilities, including contracted responsibilities and NCQA accreditation or certification requirements, [MCO will work with Delegate to create a corrective action plan to identify areas of improvement and actions plans to ensure compliance with all elements and categories. If Delegate does not take corrective action, or fails to meet improvement goals, [MCO reserves the right to revise the delegation agreement and scope, or revoke the delegation agreement all together.

**Subdelegation**

It may be allowable for a Delegate to subdelegate specific activities that relate to credentialing and recredentialing of Crisis Services providers. Subdelegation will require prior written approval by [MCO. In addition to the requirements for subdelegation set forth in the Agreement, Delegate will submit to MCO a Delegation Chart (template to be provided by [MCO). If the Delegate chooses to subdelegate any activities, the Delegate is giving the Delegate authority to perform the delegated activities. As such, the Delegate is responsible for ongoing oversight of the subdelegate's performance and is required to report performance results to [MCO.

DELEGATION GRID				
Function	Delegation Status	Delegated Activities	Reporting Data, Frequency & Submission	[MCO Activities
CR 7: Assessment of Organizational Providers	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	ALL	N/A	N/A
Decision Making	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	Agency: Approved, Denied, Terminated, Pending.  All verifications have 180 days freshness from date of decision.	At least monthly standard reporting in electronic format to designated MCO Staff/email	MCO retains the right to approve, suspend and terminate individual practitioners, providers and sites
Ongoing Monitoring	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	State Exclusion Website OIG SAM	Completed by 15 <sup>th</sup> of Month- Delegate is to maintain documentation	N/A

Disclosure and/or Ownership Form	<input checked="" type="checkbox"/> Delegated <input type="checkbox"/> Not Delegated	Collected at initial contracting and 36 months after or if any changes	N/A	If applicable to MCO

**Coordinated Care of Washington**

**SALISH BEHAVIORAL HEALTH  
ADMINISTRATIVE SERVICES  
ORGANIZATION, BY KITSAP  
COUNTY BOARD OF  
COMMISSIONERS, Its Administrative  
Entity**

Address: 1145 Broadway Ste 300  
Tacoma WA 98402

Address: 604 Division St, Ms-23  
Port Orchard, WA 98366

Phone: 877-644-4613

Phone: 800-525-5637

Email: Beth.Johnson@

Email: shew@sdc.kitsap.wa.us

CoordinatedCareHealth.com  
Signature

E. Wolfe  
Edward E. Wolfe, Chair

By: [Signature]

[Signature]  
Charlotte Garrido, Commissioner

Title: President & CEO

[Signature]  
Robert Gelder, Commissioner 8-17-19

Date: 8/15/19

ATTEST:

[Signature]  
Dana Daniels, Clerk of the Board

