AGENDA ITEM or FINAL CONTRACT REVIEW SUBMITTAL FORM

Agenda Item: Amendment No. 2; Comm. Integration Agrmt; RMHMP

Action Requested: County Manager Signature

Parties to the Agreement:

Term Begins: **Term Ends:** **Grant Contract #:**

Summary:

Ongoing integrated community care - case management -

Fiscal Impact:

Submitted by: Randy Morgan for Joni Reynolds **Submitter's Email Address:** rmorgan@gunnisoncounty.org

Finance Review: (●) Required ( ) Not Required

Comments:
No concerns, cost covered in 2020 adopted budget. ln

Reviewed by: GUNCOUNTY1\lNienhueser Discharge Date: 7/11/2020

County Attorney Review: (●) Required ( ) Not Required

Comments:
ok db 7/15/20

Reveiwed by: GUNCOUNTY1\dBaumgarten Discharge Date: 7/15/2020 Certificate of Insurance Required

Yes ( ) No (●)

County Manager Review:

Comments:

Reveiwed by: GUNCOUNTY1\emense Discharge Date: 7/17/2020

(●) Consent Agenda ( ) Regular Agenda ( ) Worksession Time Allotted: 0

Agenda Date: 7/21/2020

Revised April 2015

AMENDMENT NO. 2
TO COMMUNITY INTEGRATION AGREEMENT

This AMENDMENT NO. 2 TO COMMUNITY INTEGRATION AGREEMENT ("Amendment") is made as of May __, 2020 (the "Amendment Effective Date"), between Rocky Mountain Health Maintenance Organization, Inc.("RMHO") dba United HealthCare Services, Inc., a Minnesota corporation with offices at 9900 Bren Road East, Minnetonka, MN 55343 ("UHS"), on behalf of itself and its affiliates, and Gunnison County Department of Health and Human Services ("Vendor") with its principal offices located at 220 North Spruce St. , Gunnison, CO 81230 ("Vendor") with reference to the following facts:

Commented [MA1]: Date to be inserted by UHS when sent for signatures.

Commented [MA2]: Gunnison – Please confirm your legal business name

Commented [MA3]: Gunnison - Please confirm legal business address

A. RMHO and Vendor previously have entered into that certain Community Integration Agreement, dated January 1, 2019 (the "Agreement").

B. UHS and Vendor now desire to amend the Agreement as set forth below in this Amendment.

In consideration of the mutual promises and covenants set forth in this Amendment, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. DEFINITIONS

Terms defined in the Agreement shall have the same meaning when used in this Amendment.

2. AMENDMENT

2.1 Section 8A (Effective Date/Duration) of the Agreement is hereby deleted in its entity and replaced with the following:

> "A. Effective Date/Duration. This Agreement shall be effective as of the Effective Date set forth on the signature page of this Agreement, and shall continue in effect until December 31, 2020, unless otherwise terminated in accordance with the provisions of this Agreement."

2.2 Exhibit A (Community Integration Agreement – Scope of Services) of the Agreement is deleted in its entirety and replaced with the attached hereto Attachment 1

2.3 Exhibit E (Security – Tier 3) of the Agreement, attached hereto as Attachment 2, is hereby added and incorporated into the Agreement.

2.4 Exhibit F (Medicare Advantage Regulatory Requirements Appendix) of the Agreement, attached hereto as Attachment 3, is hereby added and incorporated into the Agreement.

2.5 Exhibit G (Master Community & State Appendix) of the Agreement, attached hereto as Attachment 4, is hereby added and incorporated into the Agreement.

3. NO OTHER CHANGES.

Except as specifically amended by this Amendment (and any other amendments executed by the parties) pursuant to Section 9I of the Agreement, the Agreement is unmodified and shall remain in full force and effect.

IN WITNESS WHEREOF, the parties have executed this Amendment by their duly authorized representatives in one or more counterparts, each of which will be deemed an original, effective as of the Amendment Effective Date.

UNITED HEALTHCARE SERVICES, INC., ON BEHALF OF ITSELF AND ITS AFFILIATES	**GUNNISON COUNTY DEPARTMENT OF HEALTH AND HUMAN SERVICES**
By: _____ (Authorized Signature)	By: _____ (Authorized Signature)
Name: _____ (Print or Type)	Name: _____ (Print or Type)
Title: _____	Title: _____
Date: _____	Date: _____

ATTACHMENT 1

Exhibit A

for Integrated Community Care Team

Prioritized Activities and Interventions for RAE Region 1 Enrollees
Regional Accountable Entity
Program Year Ending December 31, 2020

Community Integration Agreement – Scope of Services

Gunnison County Health and Human Services -Gunnison County

I. Purpose and Background

Reunion Health and RMHMO (collectively known as the Reunion Health partnership) have elected to participate in the Colorado Accountable Care Collaborative as the Region 1 Regional Accountable Entity (RAE). Integrated Community Care Teams (ICCTs) are a critical component of the Reunion Health partnership's approach, which honors local intelligence and leadership to drive community-level vision and innovation aimed at improving the health and well-being of all community Covered Persons served by Medicaid. This agreement is between RMHMO and Gunnison County Health and Human Services, known as "Contractor."

The ICCT builds capacity and infrastructure in the Health Neighborhood by providing care transitions services, care coordination and complex care management. ICCTs provide the infrastructure for the team, including a supervisor and human resources support for the team; management of payroll, benefits and compensation; access to HIPAA-secure electronic devices like computers, laptops, tablets or mobile phones; work space (if needed); compensation for mileage and other necessary and usual supports.

ICCTs are multi-disciplinary and can be comprised of a range of health professionals. The ICCT structure is flexible and can be adapted to the needs of the community being served. Additionally, ICCT staff can be located in a number of settings, including a shared administrative office space, within a community mental health center (CMHC) or primary care medical practice (PCMP) or remotely. Care coordinators meet with Covered Persons in their homes as well as safe locations, like homeless shelters, hospitals and other public meeting places, or via a telehealth tool, available to all ICCT staff.

II. Key Community Partners

The ICCT and RMHMO acknowledge and agree that, while all parties are collectively as well as independently accountable for the achievement of Accountable Care Collaborative goals, their ability to be successful does not rest solely within the scope of their respective or collective control. To that end, Contractor and RMHMO agree to collaborate actively with other organizations and resources in the community, which share responsibility for program success. These include, but are not limited to:

- Specific activities with local key health neighborhood partners including providers of physical health (PH), behavioral health (BH) and inpatient services, community organizations, etc., within the specified community. Examples include:
- Attend local Nurse Family Partnership advisory board meetings,
- Participate in Healthy Communities and RMHP quarterly meetings

- Participate in referral process with Healthy Communities
- Community Health Workers, Family Resource Center, Local Interagency Operating Groups (IOGs), Hospitals, Hub and Spoke Model for Substance Use Treatment, Local Public Health Agencies (LPHAs), Long Term Supports and Services (LTSS), CMHCs, Single Entry Points (SEPs), and Community Centered Boards (CCBs).

This agreement outlines the specific strategies and initiatives the ICCT will use to accomplish the care coordination activities described briefly above (providing care transitions services, care coordination and complex care management). Outreach to and coordination with the Health Neighborhood:

- To be successful, ICCTs will have documented as well as informal relationships with Key Community Partners in the Health Neighborhood, including other ICCTs within Region 1, and other sources for care coordination services and case management in the community. To this end, the ICCT will:

  1. Outreach to and coordinate with the key entities described above to establish a point of contact with each entity and with the ICCT.
     a. Outreach includes the following activities:
        i. Participation in relevant community efforts, including regional RMHMO initiatives, such as community corrections programs, accountable health communities model (AHCM), IOGs, etc.
        ii. Activities to engage Covered Persons using evidence-based/promising practice programs in the community to address social determinants of health (SDOH)
        iii. Identification of barriers that Covered Persons experience when accessing the Health Neighborhood and community resources

  2. Reach out to RMHMO for support in establishing more formal memorandums of understanding (MOUs) to support these relationships, as necessary.

  3. Offer to meet with and/or present to entities and providers within the Health Neighborhood to introduce the ICCT as a shared resource for the community, describe the services and supports the ICCT provides, how to refer to the ICCT, and develop collaborative processes for referrals and ongoing communication.

III. Geographic Catchment Area

1. The ICCT is responsible for the RAE Covered Persons (inclusive of RMHP Medicaid Prime Covered Persons) assigned to Region 1 in a geographic catchment area as defined by RMHMO.

2. Contractor is responsible for Covered Persons in the following

   - Gunnison Valley Family Physicians
   - Town Clinic of Crested Butte

3. If it is confirmed that a referral the Contractor receives is for a Covered Person who does not receive care within the geographically defined catchment area, then upon receiving a referral for a Covered Person, regardless of catchment area, the ICCT will assess and manage the Covered Person for immediate urgent or emergent needs prior to a warm handoff to the appropriate ICCT.

4. If the Covered Person is not eligible for Medicaid or has lost eligibility, the ICCT will assist the Covered Person with either gaining eligibility (if the Covered Person qualifies) or make best efforts to ensure a connection is made with a community partner who is able to provide care coordination for Covered Person prior to disengaging with Covered Person. In this case, the ICCT may provide care coordination Services while Medicaid eligibility is established.

5. Contractor will provide care coordination and support for Covered Persons assigned to the defined geographic catchment area but receiving care outside of the catchment area. This may include individuals receiving care outside of Region 1 in Colorado, or receiving care from an out-of-state provider.

IV. Organizational Structure

ICCTs will:

1. Establish a supervisory/management structure.

2. Multidisciplinary ICCTs will organize their work to optimize the use of each staff member's professional credentials, experience and individual skills. RMHMO prefers that the ICCT have the following skill sets within their staff and these roles may overlap:
    a. Behavioral health skilled or credentialed staff (i.e. LCSW),
    b. Physical health skilled or credentialed staff (i.e. registered nurse)
    c. Staff who have skills related to addressing SDOH (i.e. social worker),
    d. Staff who are skilled at broad outreach, including telephone outreach to support transitions of care,
    e. Staff who are skilled at supporting very complex Covered Persons.

3. Follow RMHMO Medicaid Care Coordination Policy and Procedure (See Attachment A-1) for care coordination activities including specific policies and protocols for:
    a. Receiving and processing referrals,
    b. Conducting follow up outreach calls,
    c. Complex case management screening, assessment, person centered care planning and goal setting, ongoing management and case closure due to loss of contact or completion of goals.

4. Develop strategies and workflows specific to meeting the requirements under this Agreement, including the RMHMO policies and protocol listed above.

5. Each ICCT will have a "super-user" who is an expert in the RMHMO care management documentation platform (currently Essette) and the Community Resource Network (CRN) and can support light troubleshooting and training for other ICCT staff.
    a. That person will also interact with RMHMO's Essette/CRN support when more complicated issues arise. RMHMO will provide a timely response to issues.

RMHMO will offer support in developing policies, training staff and other elements of the ICCT organizational structure upon request from ICCT.

V. Support of Key Performance Indicator (KPIs) Improvement

1. ICCT will partner with RMHMO and local community stakeholders to develop intervention ideas and workflows to influence KPIs and Behavioral Health Incentive Measures. In the event CDHCPF modifies the KPIs or Behavioral Health Incentive Measures, RMHMO will send the updated list to the ICCT.

    Key Performance Indicators (KPIs):

    A. Potentially Avoidable Costs
    B. Emergency Department (ED) Visits
    C. Behavioral Health Engagement - percent of Covered Persons who received behavioral health care
    D. Well Visits
    E. Prenatal Care

F. Annual Dental Care
G. Health Neighborhood Measure

Behavioral Health (BH) Incentive Measures:

A. Engagement in Outpatient Substance Use Disorder Treatment
B. Follow-up within 7 days of an inpatient hospital discharge for a Mental Health Condition
C. Follow-up within 7 days of an Emergency Department Visit for a Substance Use Disorder
D. Follow-up after a Positive Depression Screen
E. Behavioral Health Screening or Assessment for Children in the Foster Care System

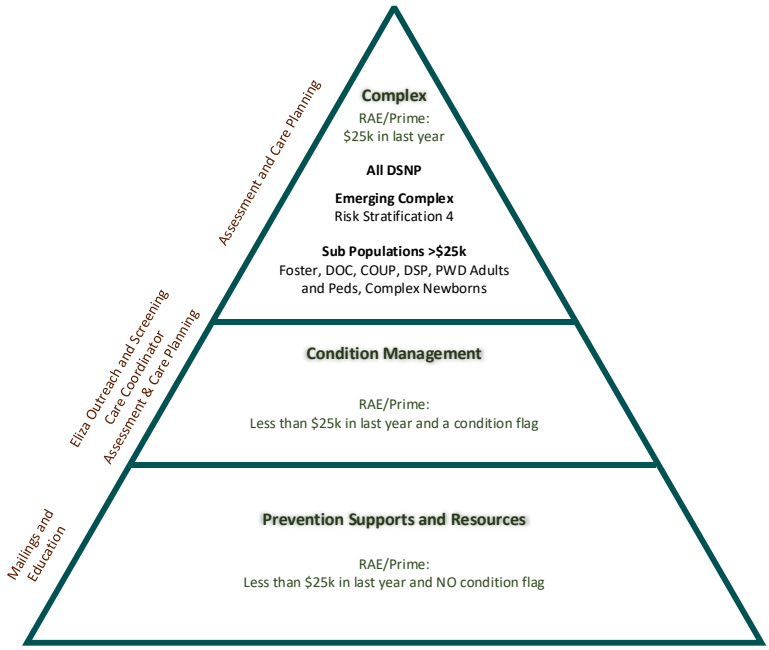
VI. Support of Risk Stratified Covered Persons

RMHMO has developed a stratification model that aligns with CDHCPF's Population Pyramid. Covered Persons have been stratified into Complex Care Management, Condition Management and Prevention Support and Resources Categories. In addition to CDHCPF's stratification, RMHMO has identified additional Covered Persons with current or emerging health risk who will benefit from care coordination.

RMHMO has used the following criteria to identify Covered Persons with Emerging Risk:

- Rx Compliance Issues: less than 60% Compliance and:
  - Lipids/Statins and in Population Health flag for Congestive Heart Failure, Ischemic Heart Disease, Myocardial Infarction or Atrial Fibrillation
- SUD
- Multiple ED Visits: 12 or more visits in 12 or less months
- Multiple Inpatient Admits: 3 or more visits in 12 months
- Behavioral Health Admission in past 12 Months
- High SDOH Issues – Covered Person has an 'SDOH' or 'AHCM' flag or Covered Person is flagged with 'High social needs' on Essette Comprehensive Assessment
- COUP, DSP, Foster Care, High Risk Pregnancy, and DOC (Special populations that are not on the State's report and that are <$25k)
- Disabled Eligibility Flag for RAE and Prime only

The following pyramid depicts the populations in the three stratifications.



Note: RMHMO will manage outreach for all Covered Persons in the Prevention Support and Resources Category.

VII.Complex and Condition Management Referral Expectations

For Covered Persons who fall into Complex and Condition Management risk categories, and will not be managed by RMHMO through a specific Complex or disease management program, RMHMO will send those Covered Persons, via referrals through Essette campaigns or via Secure email to the ICCT for outreach.

Contractor is expected to develop an extended care coordination strategy to serve the Covered Persons. Specific tools or strategies can include the following themes:

- Communication, cultural responsiveness and disability competent care,
- Proactive education promoting the effective use of Medicaid benefits,
- Training resources for care coordination staff and providers,
- Use of technology to outreach Covered Persons
- Promotion of health and wellness – engaging Covered Persons in CDHCPF's priority areas.

Contractors engaging with any Covered Person for care coordination purposes will integrate the following approaches when performing outreach activities:

1. ICCT staff will use a person- and family-centered approach to Care Coordination, which takes into consideration the preferences and goals of Covered Persons and their families, and then connects them to the resources required to carry out needed care and follow up.

2. ICCT staff will use therapeutic techniques like motivational interviewing to achieve progress and should focus on recovery and resilience and use a trauma-informed approach.

3. All Care Coordination activities must be culturally and linguistically responsive and support prevention and early intervention, where possible and appropriate.

4. ICCTs will facilitate Covered Person referrals to resources as identified through screening or assessment as it is a best practice to close the referral loop. The ICCT will follow-up with the Covered Person to determine whether the Covered Person followed through on the recommendations.

5. Covered Persons who are lower risk may request Care Coordination Services - ICCT must respond and act upon these requests as they would with complex care management.

6. ICCTs will connect Covered Persons with agencies for determination of eligibility for other available benefits and community resources (TANF, HCBS Waivers, SNAP, etc.) etc.) and utilize RMHMO as a resource to assist Covered Persons in signing up for benefits, as needed.

7. ICCTs will coordinate services across all providers within the Health Neighborhood and ICCT staff will support regular communication between care coordinators and the providers who deliver services to Covered Persons, as well as all other community partners/care coordinators involved in the Covered Person's care.

8. ICCT staff may accompany Covered Persons to appointments, supporting them to navigate health and social services when requested by the Covered Person.

9. ICCT will support Covered Persons to choose and make an appointment with a PCMP and will encourage timely preventive care, including well-child visits, immunizations, prenatal and postpartum care, annual dental visits, timely health screenings for adults.

10. Support and refer Covered Persons to current and future programs that address SDOH, Maternal Health and Newborn programs, transportation programs, AHCM referral loop closure, Community Corrections, etc.

11. Encourage and support self-management of chronic conditions, including diabetes, cardiovascular disease, congestive heart failure, mild to moderate depression and anxiety, and asthma.

12. Support and refer Covered Persons to programs designed to support special populations, like Healthy Harbors, crisis programs for intellectual or developmentally disabled individuals, programs for Covered Persons who are involved with criminal justice, etc.

13. Support and refer Covered Persons to other programs as identified by the ICCT or RMHMO.

14. It is the ICCT's responsibility to respect when a Covered Person has chosen another agency to coordinate their transitions of care and necessary for the ICCT to work collaboratively with that agency to ensure a successful transition of care. Care coordinators will make best efforts to reach out to other support systems the Covered Persons is connected with (LTSS, CCBs, etc.) and offer support.

15. ICCT will support regular communication between care coordinators and the practitioners delivering services to Covered Persons.

16. In order to support successful outreach and meet the goals set forth by CDHCPF, each ICCT needs to enhance their processes to improve extended Care Coordination activities. This may include utilizing cell phone numbers available in Essette and flexing staff hours so that staff can outreach during evening and weekend hours.

VIII. Extended Care Coordination Expectations

It is a best practice, that as much as possible, Care Coordination should take place at the point of care. ICCTs serve as practice extenders and add to the overall capacity of the Health Neighborhood to support Care Coordination for Covered Persons with Complex and Condition Management needs. As ICCTs receive referrals for these Covered Persons, there are certain expectations that RMHMO has regarding outreach.

1. Care Coordination activities are specified within the RMHMO Medicaid Care Coordination Policy and Procedure (Attachment A-1), which guides the required extended care coordination activities of each ICCT. The policy requires:

    a. Open door entry into care coordination – ICCTs must be able to accept referrals from any entity in the Health Neighborhood, such as RMHMO care management, other ICCTs, AHCM referrals, referrals from another RAE, referrals from practices and hospitals, referrals from community partners, self-referral, etc.
    b. Initial screening to determine need for services for Covered Persons who are referred to Care Coordination (through RMHMO, providers, through self-referral).
    c. A comprehensive assessment inclusive of physical, behavioral health and SDOH, cognitive and functional (activities of daily living (ADLs), and instrumental activities of daily living (IADLs)) status, and condition-specific issues, as specified by the Medicaid Assessment in RMHMO's care management platform will occur within 2 months of initial outreach. The comprehensive assessment includes documentation of clinical and behavioral health history, including medications, initial assessment of life-planning activities, evaluation of cultural and linguistic needs, preferences or limitations, evaluation of visual and hearing needs, preferences or limitations, evaluation of caregiver resources and involvement and identification of barriers to Covered Person meeting goals or complying with the case management plan.
    d. This comprehensive assessment will be face-to-face, if possible. Follow-up will occur at a minimum monthly, but as frequently as daily depending on the Covered Person's needs, both telephonically and face to face with the Covered Person, family and care team.
    e. Develop a care plan which defines care providers, supports and services currently in place, caregivers, and other appropriate service providers. Determine level of additional need to determine goals, barriers and interventions.
    f. Follow up with all Covered Persons who are on a care plan if they have had a clinical incident (ER or inpatient visit).
    g. Follow up with Covered Persons who miss specialty care appointments to ensure transportation is secure for rescheduled appointment.
    h. Appropriate case closure due to loss of contact or completion of goals.

2. All activities must be completely documented as set forth in RMHMO's documentation workflows provided during training.

3. For Covered Persons with a behavioral health issue as their primary concern, a designated staff member of the ICCT, preferably a person with a behavioral health background and training, will serve as the designated liaison and collaborate with the Covered Person and the Covered Person's preferred behavioral health provider to support the care plan developed by the behavioral health provider. If the Covered Person does not have an established relationship with a behavioral health provider, then ICCT will work with the Covered Person to establish a relationship.

4. A designated contact from RMHMO's Care Management ICCT leadership will serve as a resource for ICCTs to support case reviews, provide guidance, answer questions and coordinate needed resources. RMHMO will provide a timely response to issues.

IX. Transitions of Care

ICCTs are responsible for supporting transitions of care activities for the population in their given geographic catchment area. Transitions of care activities have timeliness and other requirements as follows:

1. Transitions of care activities will be performed for the following Covered Persons including, but not limited to, children involved with child welfare, Medicaid-eligible individuals transitioning out of the criminal justice system, Covered Persons receiving LTSS services, and Covered Persons transitioning out of institutional settings. ICCT will support transitions for Covered Persons who:
    a. Transfer from one RAE to another RAE when Covered Persons are actively engaged in Care Coordination and/or receiving covered services through the Capitated Behavioral Health Benefit.
    b. Transfer from institutional settings to community-based services.
    c. Are children involved with child welfare, children aging out of the foster/kinship care system and other targeted special populations.
    d. Are Medicaid-eligible Covered Persons transitioning out of the criminal justice system.

Activities to support transitions of care include: answering the Covered Persons questions, supporting scheduling of follow-up appointments, ensuring that home care services are established if ordered and proactively identifying and addressing risks associated with hospital readmission or avoidable ER visits and connecting with other agencies to support SDOH, BH, etc.

X. Special Populations

ICCTs are responsible for supporting RMHMO programs that address the needs of Special Populations. It is the role of the ICCT to outreach and intervene with these special populations to link them to appropriate and available services to meet their needs.

a. **Department of Corrections (DOC) Criminal Justice Transitions Program**: support them with physical, behavioral and social needs as they transition from prison back into the community
b. **Foster Care**: support them with physical, behavioral and social needs as they transition between families and once they are living with a family
c. **High Risk Pregnant Women Outreach**: support RMHMO program and work with Nurse Family Partnership to support high risk pregnant women during pregnancy
d. **Client Over-Utilization Program (COUP):**
The contractor shall review quarterly COUP report on its attributed Covered Persons, outreach to all Covered Persons on report and complete COUP report with outreach feedback by report deadline so that RMHMO can forward report to the Department.
e. **Persons With Disabilities (PWD),** adults and children, those with and without Intellectual and Developmental Disabilities (I/DD): support them with physical, behavioral and social needs; work closely with LTSS and CCBs to support persons
f. **Complex Newborns**: support family with physical, behavioral and social needs; work closely with Nurse Family Partnership and Healthy Communities to support newborns and their families

XI. Screening and Navigation for Social Determinants of Health (AHCM)

Screening and Navigation Requirements for Social Determinants of Health are specified within the AHCM Policy and Procedure, Attachment A-2, which guides the required activities of each ICCT. The policy requires:

1. Open door entry into care coordination – ICCTs must be able to accept referrals through the AHCM screening performed by practices and hospitals and work to coordinate services across all social determinants of health providers within the Health Neighborhood (food, housing, transportation etc.).

2. Follow the AHCM workflow defined in Essette and document in an AHCM Compliant way.

3. If the ICCT is also a clinical organization they must participate in the Accountable Health Communities Model as a screening organization. Contractor must have a completed AHCM MOU by February 1, 2020 and be systematically screening all Medicaid enrollees for social needs using the AHCM screening tool by March 1, 2020.

XII. Referral Protocols

1. ICCTs will be trained on and use available technology to close the referral loop, ensuring to the extent possible that the Covered Person is supported to act on the referral for services and the service provider acknowledges the referral.
2. The ICCT is encouraged to create a close-the-loop protocol in collaboration with key community partners.
3. When the ICCT receives a referral from any Health Neighborhood partner, the ICCT is required to acknowledge and respond to the referral within 2 business days.

XIII. Use of Technology and Tools

In order to support an integrated network of communication across care coordination resources throughout the region, RMHMO or its partners will provide and support shared technology. ICCTs will be trained on and adopt the following tools:

1. RMHMO Care Management platform (currently Essette) and use of Admissions, Discharge and Transfer (ADT) data.
2. CareNow- a doc or therapist on demand telehealth platform available to all RAE and Prime Covered Persons.
3. ICCTs agree to adopt future technologies designed to be non-duplicative and enhance communication across systems, the network and support services.

XIV. Training

1. RMHMO will offer the following trainings and we encourage Contractor to attend:

    a. Use of Essette & documentation Standards
    b. Transitions of Care
    c. Comprehensive Assessment
    d. Strategies for supporting high-complexity clients
    e. Bridges Out of Poverty
    f. Person centered approach to care planning and care coordination
    g. Cultural Competency
    h. Disability competency
    i. Trauma-informed care
    j. Knowledge of local resources and services
    k. Ethics
    l. Healthy Eating & Active Living and how to promote these activities with Covered Persons
    m. Stress management & self-care

n. Zero Suicide Initiative
o. Training for the 7 core competency skills: patient engagement, stages of change, Motivational Interviewing, care coordination, supporting behavior change, Adherence support, group self-management
p. Additional advanced training includes: Trans-theoretical model of stages of change, management of chronic pain, family planning and pregnancy/child development, Basic understanding of common disease processes (addiction disorders, diabetes, anxiety, depression, CV disease, etc.).

2. A trainer employed by the ICCT or by RMHMO or one of the Reunion Health partners may provide trainings. Other Community Health Neighborhood partners who provide best practices trainings may be approved.
3. RMHMO will be an ongoing resource for Essette training and support. Through the Essette platform, ICCTs will receive ADT data, care plans, assessments etc. for Covered Persons.

4. Reports are available through Essette platform for the ICCTs query that allow them to monitor their own performance under this Agreement.

XV. Reporting

1. Complex Care Management Report (Monthly):

Note: If the ICCT documents all of its Care Coordination activities in Essette, RMHMO will pull all RAE 1 Complex Care Coordination data out of that system and provide copies to the Contractor.

If the ICCT *does not* document all of its Care Coordination activities in Essette, the ICCT is required to complete RAE 1 Complex Care Management Report (see attachments A-3 and A-4)

- Complex Care Management Data will be due mid-way through the quarter. See dates below
  - SFY Q4 Data : 1.15.20
  - SFY Q1 Data : 4.15.20
  - SFY Q2 Data : 7.15.20

2. Condition Management Report

Narrative: If the ICCT has programs for any of the following conditions, the ICCT will provide a description of those programs to RMHMO

- Maternity
- Diabetes
- Hypertension
- Congestive Heart Failure/ Cardiovascular Disease (CHF/CVD)
- Asthma
- Chronic Obstructive Pulmonary Disease (COPD)
- Anxiety
- Depression
- Chronic Pain
- Substance Use Disorder

This report is due to CDHCPF biannually, so narrative will be due from ICCTs:
SFY Q1-Q2 Jul-Dec 2019: 2/1/2020
SFY Q3-Q3 Jan-June 2020: 8/1/2020

3. **COUP Report (Quarterly):**
   The Contractor shall review quarterly COUP report on its attributed Covered Persons, outreach to all Covered Persons on report and complete COUP report with outreach feedback by report deadline so that RMHMO can forward report to CDHCPF. The report is due to the CDHCPF on the 10th business day of the month following the end of the previous quarter.
   - Quarterly COUP Covered Persons Distribution: RMHMO will transmit files to ICCT either via ECG Connect or through an Essette campaign.
   - RMHMO may request a "check in" file of the quarterly COUP Covered Persons progress.
   - Completed COUP Outreach and Navigation file from Contractor will be due on the following dates:
     - SFY Q4 Data : 1.15.20
     - SFY Q1 Data : 4.15.20
     - SFY Q2 Data : 7.15.20

4. **ICCT Staffing Measures (At least annually by July 15th of each year and as changes occur:**
   a. Number of FTEs dedicated to care coordination
   b. Professional credentials of each staff Covered Person
   c. Trainings completed during the reporting period for each staff Covered Person
   d. Staff retention
      i. Staff turnover in the reporting period
      ii. Positions filled
      iii. Length of time position is open

5. **Narrative and Qualitative Reporting**
   a. Frequency: as requested
      Qualitative stories on Covered Persons who benefitted from ICCT support and examples of care coordination activities performed during the reporting period
   b. Frequency: Bi-annually
      Support RMHMO in pulling records and creating case studies for RHMMO annual HSAG audit.

XVI. Meetings & Oversight

1. **Meetings**

There will be quarterly meetings with each ICCT. The audit results performed by RMHMO Care Coordination will be shared in this meeting and not in a separate meeting.

A. These quarterly meetings will cover:
   i. Policy and Program updates
   ii. Contract requirements
   iii. Performance data
   iv. Barriers and solutions
   v. Training needs

*RMHMO may add more items to the above list and there may be some things that are tailored to each group. ICCTs can give topics of what they'd like to cover/discuss.

B. A supervisory/leadership representative from the ICCT or their designee must attend quarterly ICCT contract meeting and a quarterly Care Coordination region wide meeting
C. A supervisory/leadership representative from the ICCT or their designee must attend ad hoc care conferences with other key community partners and RMHP Care Management to problem-solve specific complex cases.

D. A supervisory/leadership representative from the ICCT or their designee must attend ad hoc meetings with RMHP care management Leadership, RMHP Community Integration Leadership to bilaterally address operational questions and concerns and to strategically plan as needed.

E. Scheduled and ad hoc meetings with ICCT and host organization leadership and/or staff Covered Persons

2. Oversight

RMHMO will oversee and monitor ICCT activities to ensure that they conform to the goals of its Care Coordination program.

RMHMO will measure the performance of the ICCTs

RMHMO will use reports we pull from Essette and those reports sent by ICCT teams who do not use Essette that measure performance and complete deliverables

3. **Audits**

A. Frequency: Annually: Audit of each ICCT by RMHMO to include review of documentation for clarity, completeness and quality including a review of Reporting as described in section XVI of this agreement

RMHMO will work with Contractor to coordinate dates and times of audits.

As a result of audits, there may be progressive corrective action as needed to correct concerns identified by RMHMO Care Management leadership.

XVII. Budget & Payment

The Contractor will hire and maintain the following positions to support coordination of care for Covered Persons in Contractors Geographic catchment area.

Position Title	Licensure	FTE	Employer
Care Coordinator		0.5	Gunnison County HHS
TOTAL:		0.5	

Contractor shall receive payment from RMHMO for the implementation and maintenance of resources required to fulfill requirements set forth in this Community Integration Agreement. This budget is inclusive of all expenses including but not limited to FTEs salary and benefits, administrative time, computer, phones and travel expenses:

1. Payment Schedule will be as follows:

Payment Dates	Payment amounts (per quarter)
March 15, 2020	$8,250.00
June 15, 2020	$8,250.00
September 15, 2020	$8,250.00

December 15, 2020	$8,250.00
Total amount payable for January 1 – December 31, 2020	$33,000.00

Payment will be contingent upon the satisfactory completion by the Contractor of milestones agreed by the parties pursuant to this Community Integration Agreement. The parties explicitly acknowledge that the Medicaid Accountable Care Collaborative Program and the RAE is a new and novel initiative, in which payment and/or enrollment levels established by the State of Colorado may be adjusted suddenly and dramatically without substantial notice. In the event that the State of Colorado makes unexpected, material reductions in RAE payment, enrollment or program requirements, RMHMO reserves the right to revise payment to Contractor hereunder commensurately. Contractor may likewise reduce the scope of services performed hereunder commensurately. The parties agree to respond collaboratively and constructively to address unexpected changes by the State of Colorado.

Attachments:

A-1 RMHMO Medicaid Care Coordination Policy and Procedure
A-2 AHCM Policy and Procedure
A-3 RAE 1 Complex Care Report
A-4 RAE 1 Condition Management Report
A-5 RAE 1 Population Health Plan

ATTACHMENT 2

EXHIBIT E
SECURITY – TIER 3

1. General Requirements and Definitions.

1.1 Security Program. Vendor shall maintain a comprehensive security program under which Vendor documents, implements and maintains the physical, administrative, and technical safeguards necessary to protect the confidentiality, integrity, availability, and security of Vendor Processing Resources and Customer Information and comply with applicable Law and the requirements of this Exhibit.

1.2 Vendor Security Contact. Vendor shall designate one or more privacy and data security contacts who are responsible for overseeing compliance with this Exhibit and provide Customer with the 24x7 contact information (including email and phone number) for these security representatives. Vendor will also identify its chief information security officer (or an equivalent individual) and maintain an up-to-date succession plan for the chief information security officer.

1.3 Policies and Procedures. Vendor shall maintain written security management policies and procedures to identify, prevent, detect, contain, and correct violations of measures taken to protect the confidentiality, integrity, availability, or security of Vendor Processing Resources and/or Customer Information. Such policies and procedures shall: (a) assign specific data security responsibilities and accountabilities to specific individual(s); (b) include a formal risk management program which includes periodic risk assessments; and (c) provide an adequate framework of controls that safeguard Vendor Processing Resources, Customer Information Systems and Customer Information. Vendor shall provide such policies and procedures to Customer for review upon Customer's request at any time during the Term.

1.4 Subcontractors. To the extent that any Vendor subcontractor accesses Customer Information Systems or creates, has access to, or receives from or on behalf of Customer any Customer Information in electronic format, Vendor shall enter into a written agreement with such subcontractor, which agreement shall incorporate all of the applicable provisions of this Exhibit.

1.5 Audit. In addition to any audit requirements set forth elsewhere in the Agreement, Vendor will provide to Customer, its auditors (including internal audit staff and external auditors), inspectors, regulators and other representatives as Customer may from time to time designate in writing, access at all reasonable times (and in the case of regulators at any time required by such regulators) to any facility or part of a facility at which either Vendor or any of its subcontractors is performing Vendor Processing or which contains Vendor Processing Resources, and to data and records relating to Vendor Processing, Vendor Processing Resources, and information security for the purpose of performing audits and inspections of Vendor and any of its subcontractors to (a) verify the integrity of Customer Information and examine the systems that process, store, secure, support and transmit Customer Information; (b) verify Vendor's and its subcontractors' compliance with the requirements of this Exhibit, and (c) review general controls and security practices and procedures. Vendor will cooperate fully with Customer or its designees in connection with audit functions and with regard to examinations by regulatory authorities. Customer's auditors and other representatives will comply with Vendor's reasonable security requirements in the performance of such audit.

1.6 Definitions. Capitalized terms defined elsewhere in the Agreement shall have the same meanings when used in this Exhibit. Capitalized terms used but not defined in this Exhibit shall have the meaning set forth below.

(a) "Customer Information" means any Confidential Information of Customer that includes or is comprised of any of the following: (i) protected health information (i.e., any information

that would be termed "protected health information" under the provisions of the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations); (ii) non-public personal information (i.e., any information that would be termed "non-public personal information" under the Federal Gramm-Leach-Bliley Act, any related state statutes, and any related federal or state regulations); (iii) personal data (i.e., any information relating to an identified or identifiable natural person, as further defined under the European Union Directive 95/46/EC and each EU member state's implementing laws, including any regulations and codes of conduct issued under such laws); (iv) cardholder data, as that term is defined in the most current version of the Payment Card Industry (PCI) Data Security Standard; or (v) other personal information (i.e., other personally identifiable information about individuals, or information that can be used to identify individuals, the disclosure and/or use of which is restricted by applicable federal or state Law, including social security numbers).

(b) "Customer Information Systems" means information systems resources supplied or operated by Customer or its contractors, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, proprietary applications, printers, and internet connectivity that are owned, controlled or administered by or on behalf of Customer.

(c) "Vendor Processing" means any information collection, storage or processing performed by Vendor or its subcontractors that: (i) directly or indirectly supports the Services or functions now or hereafter furnished to Customer; and (ii) involves the storage, processing, use or creation of, or access to, any Customer Information.

(d) "Vendor Processing Resources" means information processing resources supplied or operated by Vendor, including without limitation, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, printers, proprietary applications, Internet connectivity, printers and hard copies which are used, either directly or indirectly, in support of Vendor Processing.

2. Security Risk Assessment.

2.1 Assessment Timing. At Customer's request, Vendor shall complete a security assessment conducted by Customer's Enterprise Information Security department ("Security Assessment") (a) before the Effective Date, and (b) if Customer determines a periodic review is required to ensure Vendor's controls properly address current legal, regulatory, and security requirements, or (i) the Parties add Statements of Work for new or additional Services, (ii) Vendor makes any material change that might impact the security of Customer Information, or (iii) a Security Incident occurs. Additionally, Vendor shall periodically (no less than annually) evaluate its processes and systems to ensure continued compliance with obligations imposed by Law or contract with respect to the confidentiality, integrity, availability, and security of Customer Information and Vendor Processing Resources.

2.2 Assessment Requirements. In Customer's discretion, the Security Assessment may rely on Vendor's Independent Certification, or be in addition to such Independent Certification. As part of the Security Assessment, Vendor shall provide the full Independent Certification report, security management policies and procedures, and other information required by Customer to evidence that critical controls are in place. This documentation may be provided directly to Customer or presented over a mutually agreed-upon screen-sharing application.

2.3 Remediation Requirements. Vendor shall document the results of the Security Assessment and any self- evaluations and any remediation activities taken in response to such evaluations, and provide a copy to Customer, upon Customer's request. If the Security Assessment reveals that Vendor does not meet any of the requirements of this Exhibit or the Agreement, then applicable remediation requirements will be documented and tracked using a tool provided by Customer (e.g., a vendor portal or spreadsheet). Vendor will complete such

remediation requirements, and provide evidence of this to Customer, within the timeframe specified by Customer. Material remediation requirements may also be included in the applicable Statement of Work or attached to this Exhibit as Attachment 1.

3. Security Monitoring and Response.

3.1 General. Vendor shall maintain formal processes to detect, identify, report, respond to, Mitigate, and Remediate Security Incidents in a timely manner. Additionally, Vendor shall maintain mechanisms to capture, record, and examine information relevant to Security Incidents and other security-related events. Vendor will review these processes at least annually to ensure they are fit for purpose and adequate to meet the requirements of this Exhibit. As used herein, "Mitigate" or "Mitigation", as applicable, means Vendor has deployed security controls as necessary to reduce the adverse effects of a Security Incident to a level reasonably acceptable by Customer; and "Remediate" or "Remediation", as applicable, means that Vendor has completely resolved a Security Incident, such that the incident no longer poses a risk to Customer Information Systems or Vendor Processing Resources, as applicable.

3.2 Security Incidents – Notification. As used herein, "Security Incident" means the unauthorized access, use, disclosure, modification, or destruction of Customer Information or access to or interference with the operations of any Customer Information Systems or Vendor Processing Resources. Vendor will notify Customer by telephone and in writing within 12 hours of any Security Incident that results in, or that Vendor reasonably believes may have resulted in, unauthorized access to, modification of, or disclosure of Customer Information, Customer Information Systems or other Customer applications. Vendor shall provide Customer with a written Remediation plan within 24 hours of the Security Incident. Vendor shall send all notifications required under this Section to Customer at SIR@optum.com and by phone at 1-888-848-3375.

3.3 Security Incidents – Mitigation and Remediation. Upon becoming aware of a Security Incident, Vendor will Mitigate within 24 hours from the time Vendor becomes aware of the incident. With respect to Security Incidents that are Mitigated (but not Remediated), Vendor must Remediate such Security Incidents within five business days after being Mitigated. At Customer's sole discretion, the remediation timeframe for a Security Incident can also be conducted within a mutually agreed upon timeframe between Vendor and Customer, determined after discovery of the Security Incident.

4. Additional Baseline Security Requirements.

4.1 Change Management. In addition to any specific requirements and subject to any specific conditions set forth in the Agreement or the applicable Statement of Work, Vendor shall provide Customer with at least 90 days' prior written notice of any relevant material changes to Vendor's information technology infrastructure, facilities, or resources associated with information security governance and oversight, security, network, and infrastructure operations and any key personnel responsible for ensuring a secure environment spanning Vendor, any of its subcontractors, and Customer. Vendor shall employ reasonable processes, consistent with industry best practices, for change management, code inspection, repeatable builds, separation of development and production environments, testing plans, and code escrow. Code inspections must include a comprehensive process to identify vulnerabilities and malicious code. In addition, Vendor shall ensure that processes are documented and implemented for vulnerability management, patching, and verification of system security controls prior to their connection to production networks.

4.2 Infrastructure Protection. Vendor shall maintain industry standard controls to protect Vendor Processing Resources, including, at a minimum:

(a) Resources used for mobile access to Customer Information Systems shall be protected against attack and penetration through the use of firewalls, malware detection/prevention, and encryption;

(b) Processes to prevent, detect, and eradicate malicious code (e.g., viruses) and to notify Customer of instances of malicious code detected on Vendor Processing Resources that may affect Customer Information or Customer Information Systems; and

4.3 Risk Management.

(a) General. Vendor shall maintain appropriate safeguards and controls and exercise due diligence to protect Customer Information and Vendor Processing Resources against unauthorized access, use, and/or disclosure, considering all of the factors and/or requirements listed below. In the event of any conflict or inconsistency between relevant requirements, Vendor shall protect the Customer Information and Vendor Processing Resources in accordance with the most-stringent applicable requirement:

(i) Federal and state legal and regulatory requirements;
(ii) Information technology and healthcare industry best practices (e.g., HITRUST);
(iii) Customer's data security requirements, as set forth in this Exhibit, the due diligence process and/or in the Agreement; and
(iv) Any further information security requirements which are included in a Statement of Work or equivalent document which is attached to or relates to the Agreement.

(b) Patch Management. Vendor shall ensure that appropriate patches and security updates are applied in accordance with original equipment manufacturer recommendations or industry standards and best practices. Vendor shall provide process documentation to Customer upon Customer's request.

4.4 Personnel. As used herein, "Vendor Personnel" means employees, contractors or agents of Vendor, or of its subcontractors, who provide Services (or any component thereof) to Customer. Vendor shall require that Vendor Personnel who have, or may be expected to have, access to Customer Information or Customer Information Systems comply with the provisions of the Agreement, including this Exhibit. Vendor shall maintain processes for authorizing and supervising Vendor Personnel and for monitoring access to Customer Information, Customer Information Systems and/or Vendor Processing Resources. Vendor shall maintain a sanction policy to address violations of Vendor's internal security requirements or the requirements of this Exhibit. Vendor will remain responsible for any breach of this Exhibit by Vendor Personnel. Vendor shall ensure that Vendor Personnel remain aware of industry standard security practices, and their responsibilities for protecting the Customer Information. Vendor shall provide information security awareness training and education to all Vendor Personnel upon hire (or assignment to Customer's account) and annually thereafter. Such information security awareness education and training shall address the responsibilities related to the Services provided to Customer. Participation in such training by Vendor Personnel shall be mandatory and Vendor shall track attendance and, at Customer's request, provide a confirmation that all Vendor Personnel have completed such training. Vendor's information security awareness training shall include, but not be limited to:

(a) Protection against malicious software (such as viruses);

(b) Appropriate password protection and password management practices;

(c) Appropriate use of workstations and computer system accounts;

(d) HIPAA and HITECH requirements, including the Privacy Rule and Security Rule;

(e) Vendor's information security policies;

(f) Any applicable acceptable use policies;

(g) Relevant obligations set forth in the Agreement; and

(h) Procedures for reporting Security Incidents.

4.5 Physical Security. Vendor shall maintain appropriate physical security controls (including facility and environmental controls) to prevent unauthorized physical access to Vendor Processing Resources and areas in which Customer Information is stored or processed. Where practicable, this obligation shall include controls to physically protect hardware (e.g., lockdown devices). Vendor shall adopt and implement a written facility security plan which documents such controls and the policies and procedures through which such controls will be maintained.

4.6 Data and Communications Security.

(a) Exchange of Customer Information. Vendor shall utilize a method of transmitting Customer Information electronically that limits the unauthorized access to and/or modification of such information.

(b) Data Retention. Vendor shall not retain any Customer data following completion of the applicable Services, except to the extent (a) required by Law, (b) required pursuant to Exhibit F (Medicare Advantage Regulatory Requirements Appendix), or (c) expressly required by Customer in writing. Subject to the foregoing, Vendor shall ensure that following the completion of the applicable Services, the Customer data used in connection with such Services is Securely Deleted in accordance with Vendor's records retention policy, which shall be developed by Vendor and reviewed by Customer. At Customer's request, Vendor shall certify to Customer in writing that all Customer data has been destroyed as required hereunder. As used herein, "Securely Deleted" (or "Securely Delete") means that (i) hard copy materials are destroyed and cannot be reconstructed (e.g., shredded); (ii) electronic files are deleted and overwritten to a level sufficient to ensure that they cannot be retrieved or reconstructed and that any Customer data contained in the files is rendered unreadable, unusable and indecipherable; and (iii) Vendor Processing Resources are physically destroyed, degaussed or overwritten in accordance with NIST Special Publication 800-88. Vendor shall Securely Delete any Customer data provided by Customer but not required by Vendor for performance of the applicable Services promptly after Vendor discovers that such data is not needed, provided, however, that if such prompt deletion would require Vendor to reallocate resources and impact Vendor's ability to meet Service Level requirements or deadlines established by Customer, then Customer and Vendor will work together to establish a schedule for such deletion.

(c) Encryption. Vendor shall ensure that all Customer data containing Customer Information whether stored (i.e., "data at rest") or that Vendor transmitted (i.e., "data in motion") over the public internet is encrypted using valid encryption processes or processes required by the Customer, whichever is more restrictive.

(d) Protection of Systems, Devices and Storage Media. Vendor shall ensure all reasonable, industry-standard measures are taken to physically secure Vendor Processing Resources to prevent any unauthorized disclosure while in transit and while at rest. Vendor shall ensure that all Customer Information on Vendor Processing is Securely Deleted before they are used for any other purpose. All media on which Customer data is stored shall be protected against unauthorized access or modification. Vendor shall maintain reasonable and appropriate processes and mechanisms to maintain accountability and tracking of the receipt, removal and transfer of Vendor Processing Resources.

(e) Personal Devices and Removable Media. Vendor shall ensure the Vendor Personnel will not be permitted to, and will not, utilize personal computing equipment for accessing Customer Information Systems or processing Customer Information. Vendor shall prohibit Customer data from being sent via social media, personal email accounts, or non-approved medium of

communication. Vendor may not (and shall cause Vendor Personnel to not) use any such removable media to store or transfer Customer Information without Customer's prior written approval.

(f) Data Integrity. Vendor shall maintain processes to prevent unauthorized or inappropriate modification of Customer Information, for both data in transit and data at rest.

4.7 Access Control.

(a) Account Administration. Vendor shall maintain appropriate processes for requesting, approving, and administering accounts and access privileges for Vendor Processing Resources and Customer Information. These processes shall be required for both Customer-related accounts and Vendor's internal accounts for Vendor Processing Resources, and shall include procedures for granting and revoking emergency access to Vendor Processing Resources and Customer Information. All access by Vendor Personnel to Customer Information Systems shall be subject to prior approval by Customer and shall follow Customer standard policies and procedures.

(b) Access Control. Vendor shall maintain appropriate access control mechanisms to prevent all access to Customer Information and/or Vendor Processing Resources, except by (a) specified users expressly authorized by Customer and (b) Vendor Personnel who have a "need to access" to perform a particular function in support of Vendor Processing. The access and privileges granted shall be limited to the minimum necessary to perform the assigned functions. Vendor shall maintain processes to ensure that Vendor Personnel access to Customer Information is revoked no later than two business days upon termination and immediately in the case of involuntary termination.

(c) Access to Customer Information Systems. Vendor shall only have access to Customer Information Systems authorized by Customer and shall use such access solely for providing Services to Customer. Vendor shall not attempt to access any applications, systems or data which Customer has not authorized Vendor to access or which Vendor does not need to access in order to perform Services for Customer. Vendor further agrees to access such applications, data and systems solely to the extent minimally necessary to provide Services to Customer. Vendor's attempt to access any applications, data or systems in violation of the terms in this Section shall be a material breach of the Agreement. If Vendor Personnel change roles or for any other reason no longer require access to Customer Information Systems, Vendor will notify Customer within three business days. In the case of involuntary termination, Vendor will notify Customer within 24 hours.

4.8 Software Development. To the extent that services include the development of software product(s), including web applications, for customer, such software shall be developed and maintained in accordance with the development methodology specified by customer. Such software shall satisfy the appropriate customer information security policies and guidelines that are furnished by customer to vendor (which are incorporated herein by reference). Vendor shall comply with any instructions, guidelines or minimum compliance controls that are furnished by customer to vendor (which are incorporated herein by reference) to enable customer to comply with sox and/or other applicable laws. To the extent that vendor uses internally-developed software or web applications to provide the services, even if such items are not developed exclusively for customer, then (a) vendor shall insure that such items comply with any instructions, guidelines or minimum compliance controls that are furnished by customer to vendor (which are incorporated herein by reference) to enable customer to comply with applicable laws, and (b) vendor will provide customer with such information as is reasonably necessary for customer to confirm that applicable compliance controls are in place.

Attachment 1
Additional Requirements

1. Remediation Requirements.

#	Remediation Requirement	Completion Criteria	Implementation Date
	Requirements detailed in Section 1: Independent Certification Details are in place		12/31/20

Commented [MA4]: Gunnison - Please confirm you can meet this date.

ATTACHMENT 3

EXHIBIT F
MEDICARE ADVANTAGE REGULATORY REQUIREMENTS APPENDIX
VENDOR – DELEGATED ENTITY

THIS MEDICARE ADVANTAGE REGULATORY REQUIREMENTS APPENDIX (this "Exhibit") supplements and is made part of the Agreement.

SECTION 1
APPLICABILITY

This Exhibit applies to the administrative services performed and products provided by Vendor pursuant to the Agreement as such services and products relate to Medicare Advantage Benefit Plans. In the event of a conflict between this Exhibit and other appendices or any provision of the Agreement, the provisions of this Exhibit shall control except: (1) with regard to Benefit Plans outside the scope of this Exhibit; or (2) as required by applicable law.

SECTION 2
DEFINITIONS

For purposes of this Exhibit, the following terms shall have the meanings set forth below.

2.1 **Benefit Plan:** A certificate of coverage, summary plan description, or other document or agreement, whether delivered in paper, electronic, or other format, under which a Payer is obligated to provide coverage of Covered Services for a Customer.

2.2 **CMS Contract:** A contract between the Centers for Medicare & Medicaid Services ("CMS") and a Medicare Advantage Organization for the provision of Medicare benefits pursuant to the Medicare Advantage Program under Title XVIII, Part C of the Social Security Act.

2.3 C**overed Service:** A health care service or product for which a Customer is entitled to receive coverage from a Payer, pursuant to the terms of the Customer's Benefit Plan with that Payer.

2.4 **Customer:** For the purposes of this Exhibit, Customer means a person eligible and enrolled to receive coverage from a Payer for Covered Services.

2.5 **Medicare Advantage Benefit Plans:** Benefit Plans sponsored, issued or administered by a Medicare Advantage Organization as part of the Medicare Advantage program or as part of the Medicare Advantage program together with the Prescription Drug program under Title XVIII, Part C and Part D, respectively, of the Social Security Act (as those program names may change from time to time).

2.6 **Medicare Advantage Customer or MA Customer:** A Customer eligible for and enrolled in a Medicare Advantage Benefit Plan that is covered under the Agreement.

2.7 **Medicare Advantage Organization or MA Organization:** For purposes of this Exhibit, MA Organization is: (a) UnitedHealthcare Insurance Company or one of its affiliates that has entered into a contract with CMS for the purpose of offering a Benefit Plan to MA Customers; or (b) Payer.

2.8 **Payer:** An entity obligated to a Customer to provide reimbursement for Covered Services under the Customer's Benefit Plan.

SECTION 3
DELEGATED ACTIVITIES

3.1 **MA Organization Accountability; Delegated Activities.** Vendor acknowledges and agrees that MA Organization oversees and is accountable to CMS for any functions and responsibilities described in the CMS Contract and applicable Medicare Advantage regulations, including those that MA Organization has delegated to Vendor under the Agreement. In addition to the other provisions of this Exhibit, the following shall apply with respect to any functions and responsibilities under the CMS Contract that MA Organization has delegated to Vendor pursuant to the Agreement:

(a) Vendor shall perform or arrange for the provision of those delegated activities set forth in the Agreement.

(b) Vendor shall comply with any reporting responsibilities as set forth in the Agreement.

(c) If MA Organization has delegated to Vendor any activities related to the credentialing of health care providers, Vendor must comply with all applicable CMS requirements for credentialing, including but not limited to the requirement that the credentials of medical professionals must either be reviewed by MA Organization, or the credentialing process must be reviewed, preapproved, and audited on an ongoing basis by MA Organization.

(d) If MA Organization has delegated to Vendor the selection of health care providers to be participating providers in MA Organization's Medicare Advantage network, or the selection of contractors or subcontractors to perform services under the CMS Contract, MA Organization retains the right to approve, suspend or terminate the participation status of such health care providers and the agreements with such contractors or subcontractors.

(e) Vendor acknowledges that MA Organization shall monitor Vendor's performance of delegated activities on an ongoing basis. Such monitoring activities may include site visits and periodic audits. If CMS or MA Organization determines that Vendor has not performed satisfactorily, or has failed to meet all reporting and disclosure requirements in a timely manner, MA Organization may revoke any or all of the delegated activities and reporting requirements. Vendor shall cooperate with MA Organization regarding the transition of any delegated activities or reporting requirements that have been revoked by MA Organization.

SECTION 4
VENDOR REQUIREMENTS

4.1 **Data.** Vendor shall submit to MA Organization risk adjustment data as defined in 42 CFR 422.310(a) if applicable. By submitting data to MA Organization, Vendor represents to MA Organization, and upon MA Organization's request, shall certify in writing, that the data is accurate, complete, and truthful, based on Vendor's best knowledge, information and belief.

4.2 **Customer Protection.** Vendor agrees that in no event, including but not limited to, non-payment by Vendor or MA Organization, insolvency of Vendor or MA Organization, or breach of the Agreement, shall Vendor bill, charge, collect a deposit from, seek compensation, remuneration or reimbursement from, or have any recourse against any MA Customer or person (other than MA Organization) acting on behalf of the MA Customer for any fees that are the legal obligation of MA Organization under the CMS Contract.

4.3 **Eligibility.** Vendor agrees to immediately notify MA Organization in the event Vendor is or becomes excluded from participation in any federal or state health care program under Section 1128 or 1128A of the Social Security Act. Vendor shall not employ or contract for the provision of health care services, utilization review, medical social work or administrative services and products, (collectively "Eligibility Services"), with or without compensation,

with any individual or entity that is or becomes excluded from participation in any federal or state health care program under Section 1128 or 1128A of the Social Security Act. Vendor shall review the (1) Department of Health and Human Services Officer of Inspector General List of Excluded Individuals and Entities and (2) the System for Award Management (SAM), a portal for the Federal Procurement System, (and any successor lists) prior to the hiring or contracting of any new employee, temporary employee, volunteer, consultant, governing body member or subcontractor for the provision of Eligibility Services. Vendor must continue to review these lists on a monthly basis thereafter to ensure that none of these persons or entities are excluded or become excluded from participation in federal programs.

4.4 **Laws.** Vendor shall comply with all applicable federal and Medicare laws, regulations, and CMS instructions, including but not limited to: (a) federal laws and regulations designed to prevent or ameliorate fraud, waste, and abuse, including but not limited to, applicable provisions of federal criminal law, the False Claims Act (31 U.S.C. §3729 et seq.), and the anti-kickback statute (§1128B of the Social Security Act); and (b) HIPAA administrative simplification rules at 45 CFR Parts 160, 162, and 164.

4.5 **Federal Funds.** Vendor acknowledges that MA Organization receives federal payments under the CMS Contract and that payments Vendor receives from or on behalf of MA Organization are, in whole or in part, from federal funds. Vendor is therefore subject to certain laws that are applicable to individuals and entities receiving federal funds.

4.6 **CMS Contract.** Vendor shall perform the services and provide the products set forth in the Agreement in a manner consistent with and in compliance with MA Organization's contractual obligations under the CMS Contract.

4.7 **Records.**

(a) Maintenance; Privacy and Confidentiality; Customer Access. Vendor shall maintain records and information related to services performed and products provided by Vendor under the Agreement, in an accurate and timely manner. Vendor shall maintain such records for the longer of the following periods:

(i) in the case of records containing information related to the medical loss ratio information reported to CMS by the MA Organization, including, for example, information related to incurred claims and quality improvement activities, at least ten (10) years from the date such medical loss ratio information is reported to CMS by the MA Organization, or

(ii) in the case of all records, at least ten (10) years from the final date of the CMS Contract period in effect at the time the records were created, or such longer period as required by law.

Vendor shall safeguard MA Customer privacy and confidentiality, including but not limited to the privacy and confidentiality of any information that identifies a particular MA Customer, and shall comply with all federal and state laws regarding confidentiality and disclosure of medical records or other health and enrollment information, including the requirements established by MA Organization and the Medicare Advantage program, as applicable.

(b) Government Access to Records. Vendor acknowledges and agrees that the Secretary of Health and Human Services, the Comptroller General, or their designees shall have the right to audit, evaluate and inspect any pertinent books, contracts, computer or other electronic systems (including medical records), patient care documentation and other records and information belonging to Vendor that involve transactions related to the CMS Contract. This right shall extend through the longer of the following periods:

(i) in the case of records containing information related to the medical loss ratio information reported to CMS by the MA Organization, including, for example, information related to incurred claims

and quality improvement activities, at least ten (10) years from the date such medical loss ratio information is reported to CMS by the MA Organization, or

(ii) in the case of all records, at least ten (10) years from the later of the final date of the CMS Contract period in effect at the time the records were created or the date of completion of any audit, or longer in certain instances described in the applicable Medicare Advantage regulations.

For the purpose of conducting the above activities, Vendor shall make available its premises, physical facilities and equipment, records relating to the services performed and the products provided under the Agreement, and any additional relevant information CMS may require.

(c) MA Organization Access to Records. Vendor shall grant MA Organization or its designees such audit, evaluation, and inspection rights identified in subsection 4.7(b) as are necessary for MA Organization to comply with its obligations under the CMS Contract. Whenever possible, MA Organization will give Vendor reasonable notice of the need for such audit, evaluation or inspection, and will conduct such audit, evaluation or inspection at a reasonable time and place.

4.8 **Subcontracts.** If Vendor has any arrangements, in accordance with the terms of the Agreement, with affiliates, subsidiaries or any other subcontractors, directly or through another person or entity, to perform any of the services or provide any products Vendor is obligated to perform or provide under the Agreement that are the subject of this Exhibit, Vendor shall ensure that all such arrangements are in writing, duly executed, and include all the terms contained in this Exhibit. Vendor shall provide proof of such to MA Organization upon request. In addition, Vendor agrees to oversee and monitor, on an ongoing basis, the services Vendor has subcontracted to another person or entity. Vendor further agrees to promptly amend its agreements with such subcontractors, in a manner consistent with the changes made to this Exhibit by MA Organization, to meet any additional CMS requirements that may apply to the performance of the services or the provision of the products.

4.9 **Offshoring.** Unless previously authorized by MA Organization in writing, all services provided by Vendor pursuant to the Agreement that are subject to this Exhibit must be performed within the United States, the District of Columbia, or the United States territories.

If MA Organization authorizes Vendor in writing to perform Medicare-related services that involve Medicare beneficiary protected health information ("PHI") pursuant to the Agreement at locations outside of one of the fifty United Sates, the District of Columbia, or one of the United States Territories (American Samoa, Guam, Northern Marianas, Puerto Rico and Virgin Islands), the following provisions apply:

(a) Vendor represents and warrants to MA Organization that Vendor has in place and will comply with policies and procedures to ensure that all PHI and other personal information remains secure. Vendor will provide written evidence of the policies and procedures upon MA Organization's request.

(b) Vendor will provide prior written notice to MA Organization of (a) any material change in the Medicare-related services that involve PHI that Vendor performs offshore, (b) any material change in Vendor's policies and procedures to ensure that all PHI and other personal information remains secure, and (c) any material change in the tools and systems used by Vendor to ensure that all PHI and other personal information remains secure.

(c) Vendor is prohibited from receiving access to any PHI or other personal information that is not associated with its contractual relationship with MA Organization. If Vendor receives access to PHI or other personal information of MA Organization's members that is not associated with Vendor's contractual relationship with MA Organization, Vendor will immediately notify MA Organization that it has received such access, return all PHI or personal information accessed by Vendor, and destroy any such PHI or personal information that remains in Vendor's possession after doing so (i.e. copies, electronic records, back-ups or temporary files).

(d) Vendor's services under the Agreement may be terminated immediately upon discovery of a significant security breach.

(e) Vendor authorizes MA Organization or its designee to conduct an audit of Vendor at least annually.

(f) Vendor acknowledges and agrees that MA Organization will use the results of its audit of Vendor to evaluate the continuation of MA Organization's relationship with Vendor.

(g) Vendor authorizes MA Organization or its designee to share the results of audits of Vendor with CMS.

SECTION 5
OTHER

5.1 **Regulatory Amendment.** MA Organization may unilaterally amend this Exhibit to comply with applicable laws and regulations and the requirements of applicable regulatory authorities, including but not limited to CMS. MA Organization shall provide written notice to Vendor of such amendment and its effective date. Unless such laws, regulations or regulatory authority(ies) direct otherwise, the signature of Vendor will not be required in order for the amendment to take effect.

rev. 08-13

ATTACHMENT 4

EXHIBIT G
MASTER COMMUNITY & STATE APPENDIX

THIS MASTER COMMUNITY & STATE APPENDIX (this "Exhibit") supplements and is made part of the Agreement. This Exhibit applies with respect to the provision of services Vendor provides for any Customer health plan Affiliate administering a Medicaid or other state-specific ("State") government funded and regulated program ("State Program"). In the event of a conflict between this Exhibit and other appendices or any provision of the Agreement, the provisions of this Exhibit shall control except with regard to benefit plans outside the scope of this Exhibit or unless otherwise required by law or applicable State regulatory agency. Vendor will comply with the following requirements to the extent applicable to Vendor's performance of services under the Agreement. Capitalized terms used but not defined in this Exhibit shall have the meaning assigned to them in the Agreement or other applicable appendix.

1. Regulatory Approval and Filing. In the event Customer is required to file the Agreement with federal, state or local governmental authorities, Customer shall be responsible for filing the Agreement with such authorities as required by any applicable law or regulation. If following any such filing, the governmental authority requests changes to the Agreement, Vendor agrees to cooperate with Customer in preparing the response to the governmental authority.

2. Compliance with Law and Government Contracts. Vendor and Customer agree to comply with all applicable federal, State, and local laws, rules, and regulations in connection with the performance of their obligations under the Agreement. All tasks under the Agreement also must be performed in accordance with the requirements of applicable contracts between any Customer Affiliate and State and/or federal regulatory agencies. Customer will provide or otherwise communicate such requirements to Vendor. Vendor shall ensure all agents, employees, assigns and subcontractors, if any, that are involved in providing services under the Agreement also comply with this Section.

3. Delegation and Oversight. In compliance with the delegation and oversight obligations imposed on Customer Affiliates under their contracts with State and/or federal regulatory agencies, Customer reserves the right to revoke any functions or activities delegated to Vendor under the Agreement, if in the reasonable judgment of Customer or an applicable Customer Affiliate, Vendor's performance under the Agreement does not comply with obligations under applicable government contracts. This right shall be in addition to Customer's termination rights under the Agreement.

4. Press Release; Marketing; Advertising; Use of Name and Trademarks. Except as otherwise set forth in the Agreement, Vendor shall not publicly use the name, logo, trademark, trade name, or other marks of Customer without Customer's prior written consent. The parties mutually agree to provide, at a minimum, at least 48 hours advance notice and opportunity to comment on all press releases, advertisements or other media statements and communications regarding the Agreement, the services or the business relationship between the parties. A party shall obtain the other party's written consent prior to any publication or use of such materials or communications. Nothing herein shall be construed to create a right or license to make copies of any copyrighted materials.

5. Offshoring. Unless previously authorized in writing by the appropriate Customer health plan Affiliate and State governing agency, if required, all work performed under the Agreement shall be performed from location(s) in the 50 United States. If Vendor receives authorization pursuant to this Section 5 to offshore certain obligations under the Agreement, Customer will provide, and Vendor shall comply with, all applicable offshoring regulations, requirements or restrictions, including any applicable security controls. The parties agree that any offshoring restrictions or requirements may be updated at any time to comply with applicable law and any other requirements.

6. Subcontracts. To the extent required by any regulatory agency governing any Medicare or Medicaid or other governmental benefit plans (or as may be set forth in an appendix) or any accrediting agency, Vendor shall provide advance notice to Customer and obtain Customer's consent prior to any subcontracting of any of its responsibilities under the Agreement.

7. Regulatory Amendment. Customer may unilaterally amend this Exhibit to comply with applicable regulatory requirements required under law. Upon Customer's notification of such changes, Customer will provide notice to Vendor. If such regulatory amendment materially affects the position of either party or renders it illegal for a party to continue to perform under the Agreement in a manner consistent with the parties' intent, then the parties shall negotiate further amendments to this Exhibit or the Agreement as necessary to correct any inequities, to the greatest extent possible.

8. Excluded Individuals and Entities. Vendor agrees to immediately notify Customer in the event Vendor is or becomes debarred, suspended or excluded from participation in any federal or state health care program under Section 1128 or 1128A of the Social Security Act. Vendor shall not employ or contract for the provision of services under the Agreement, with or without compensation, with any individual or entity that is or becomes debarred, suspended or excluded from participation in any federal or state health care program under Section 1128 or 1128A of the Social Security Act. Vendor shall review: (1) the Department of Health and Human Services Officer of Inspector General List of Excluded Individuals and Entities; (2) the System for Award Management (SAM), a portal for the Federal Procurement System and (3) the applicable State Programs exclusion lists, (and any successor lists) prior to the hiring or contracting of any new employee, temporary employee, volunteer, consultant, governing body member or subcontractor for the provision of services under the Agreement. Vendor must continue to review these lists on a monthly basis thereafter to ensure that none of these persons or entities are or become debarred, suspended, or excluded from participation in federal programs of State Programs.

9. Effect of Termination or Expiration. Within 30 days after the expiration or termination for any reason (or to any extent) of the Agreement and/or this Exhibit, Vendor shall return or destroy all applicable PHI, if feasible to do so, including all applicable PHI in possession of Vendor's agents or subcontractors. To the extent return or destruction of the PHI is not feasible, Vendor shall notify Customer in writing of the reasons return or destruction is not feasible and, if Customer agrees, may retain the PHI subject to this section. Under any circumstances, Vendor shall extend any and all protections, limitations and restrictions contained in this Exhibit to Vendor's use and/or disclosure of any applicable PHI retained after the expiration or termination (to any extent) of the Agreement and/or this Exhibit, and shall limit any further uses and/or disclosures solely to the purposes that make return or destruction of the PHI infeasible.