2024 Annual SHARE Initiative Spending Plan Template

Due: December 31, 2024

Overview

The SHARE Initiative (Supporting Health for All through Reinvestment) was created through Oregon House Bill 4018 (2018). It requires coordinated care organizations (CCOs) to invest a portion of profits back into communities to address health inequities and the social determinants of health and equity (SDOH-E). For details, see OHA's SHARE Initiative guidance document. SHARE Initiative guidance is posted to the SHARE Initiative webpage.

Per the requirements stated in ORS 414.572(1)(b)(C) and OAR 410-141-3735, CCOs must designate a portion of annual net income or reserves that exceed the financial requirements for SHARE Initiative spending. CCOs are subject to a formula that determines their required minimum SHARE obligation. CCOs will follow the instructions in the Exhibit L6.7 financial reporting template to apply this formula to their 2023 financials and report their 2024 SHARE designation.

The CCO contract requires a CCO's annual SHARE Initiative designation to be spent down within three years of OHA's approval of the same year's SHARE Initiative spending plan; a one-year extension may be requested (four years total).

SHARE Initiative spending must meet the following four requirements:

1. Spending must fall within SDOH-E domains and include spending toward a statewide housing priority;
2. Spending priorities must align with community priorities from community health improvement plans;
3. A portion of funds must go to SDOH-E partners; and
4. CCOs must designate a decision-making role for the community advisory council(s) related to its SHARE Initiative funds.

(See OHA's SHARE Initiative guidance document for more details.)

It is important to note that SHARE Initiative reinvestments must go toward upstream, non-health care factors that impact health (for example, housing, food, transportation, educational attainment or civic engagement).

By December 31 of each contract year, the CCO shall submit a SHARE Initiative Spending Plan to OHA for review and approval. The spending plan will identify how the CCO intends to direct its SDOH-E spending based on net income or reserves from the prior year for the SHARE Initiative. This annual SHARE Initiative spending plan will capture from CCOs how they are meeting these contractual requirements.

SHARE Initiative Reporting

A. By June 30, each CCO must report its
   - **Annual SHARE Initiative Designation** in Exhibit L, Report L6.7 to identify its SHARE Initiative designation based on the *prior year's financials*.
   - **Annual SHARE Initiative Spend-Down** in Exhibit L, Report L6.71 to track year-over-year SHARE spending and to tie such spending to the appropriate year's SHARE Initiative Spending Plan.
   - **Annual SHARE Detailed Spending** in Exhibit L, Report 6.71 to track spend-down to each SDOH-E partner each year.

B. By December 31, each CCO must complete the **Annual SHARE Initiative Spending Plan** described in this document for the *prior year's financials*.

2024 SHARE Initiative Spending Plan Template

CCO name: Trillium Community Health Plan Southwest

CCO contact: Dominique Lopez-Stickney

Instructions:

- Respond to items 1–9 below using this template.
- Be clear and concise.
- CCOs no longer need to submit partner agreements to OHA. CCOs still must have partner agreements in place that include all elements outlined in guidance prior to disbursing funds.
- Use clear file names (for example, CCOname-SHARE-Spending-Plan-2024).
- Submit your plan in the CCO Contract Deliverables Portal by December 31. (The submitter must have an OHA account to access the portal.)

Section 1: SHARE Initiative Designation

1. **What is the dollar amount of your CCO's SHARE Initiative designation represented in this spending plan? This amount must meet or exceed your CCO's designation amount recorded in cell G40 in Exhibit L – *Report L6.7.* If the amount does not match, please explain.**
   $2,398,905

Section 2: SHARE Initiative Spending Plan

Spending plan project summaries

2. **Provide a summary of the work your CCO is funding through this year's SHARE Initiative. Duplicate the row below and complete it for each funded project included in your spending plan.** Note: SHARE funds may not be used for any covered Medicaid benefits or delivery of covered Medicaid benefits, including health-related social needs (HRSN) covered services and substance use disorder (SUD) covered services.

Project #	Project name	Brief project description, including project goals, objectives and expected outcomes	Is this a housing project? If yes, indicate project type.[1]	SDOH-E domain	Populations served (list)[2]
1	Trillium Produce Plus; Trillium Veggie Rx	Trillium Produce Plus: provides fresh fruits and vegetables in clinics, schools, community-based organizations, and public distribution sites. Measurable outcomes are number of individuals served, and amount of food distributed. Trillium Veggie Rx in association with FOOD for Lane County Youth Farm: program focuses on a specific Trillium member demographic each year. In	☐ Housing services and supports ☐ Permanent supportive housing ☐ Other (write in; for example, transitional housing, emergency shelter, affordable housing):	☒ Neighborhood and built environment ☐ Economic stability ☐ Education ☐ Social and community health	American Indian and Alaskan Native, Rural, LGBTQ+, families with children, seniors, students, neighborhood

[1] For definitions of "housing services and supports" and "permanent supportive housing," see the SHARE guidance document.
[2] If applicable, please use standardized race, ethnicity, language and disability (REALD) categories (see REALD form).

		2024, the population is the Start Smart for Baby participants. Members will be screened for HRSN eligibility first. Measurable outcomes are number of Trillium members served by Veggie Rx and number of produce boxes distributed.			s with high food insecurity. Members enrolled in Start Smart for Baby and not HRSN eligible for Nutrition.
2	Families Annex Kitchen; First Place Day Care; Pallet Shelters	Families Annex Kitchen: capital improvements to the kitchen that will serve up to 22 families per day who reside at the Annex. First Place Day Care: accessible program designed to support families experiencing homelessness staying at the Annex. The current program model includes four areas of service: a therapeutic preschool, family resource referrals, family support activities, and community engagement. It will serve 32 children. Pallet Shelters: these shelters are located at the Annex and will provide emergency shelter with a capacity to house six families at a time.	☐ Housing services and supports ☐ Permanent supportive housing ☒ Other (write in; for example, transitional housing, emergency shelter, affordable housing): Emergency shelter	☒ Neighborhood and built environment ☒ Economic stability ☒ Education ☐ Social and community health	Members who are experiencing homelessness
3	HRSN Housing Implementation Process Mapping	Facilitation of workshops will help define community partner roles; capture themes; meeting outcomes; and develop process maps that will help to build structure around how 1115 housing waiver benefit is operationalized. Additionally, themes, conclusions, and process flows will be completed following the facilitation of the meeting series. Expected outcomes are the completion of process maps at the end of the end of the project.	☒Housing services and supports ☐ Permanent supportive housing ☐ Other (write in; for example, transitional housing, emergency shelter, affordable housing):	☐ Neighborhood and built environment ☒ Economic stability ☐ Education ☐ Social and community health	Populations served by the 1115 Waiver for those at risk of homelessness starting on 11/1, and additional Focus Populations once the Waiver is fully implemented.
4	Houseless Diversion and Rapid Rehousing for Non-HRSN Eligible	Housing supports for members who we have received a referral to the CCO but are not eligible for HRSN housing supports. Supports include rent, utilities, fees, deposits, education, and support services. 55	☒Housing services and supports ☐ Permanent supportive housing ☐ Other (write in;	☐ Neighborhood and built environment ☒ Economic stability	Members referred for HRSN and do not meet eligibility.

	Members	families will maintain or secure housing through this program.	for example, transitional housing, emergency shelter, affordable housing):	☐ Education ☐ Social and community health	
5	FUSE Program	The FUSE (Frequent Users Systems Engagement) program identifies and helps participants address barriers to housing; provides case management, connects participants to community resources, supportive housing placements that help minimize participants' utilization of crisis services. Desired outcomes are decrease in cost, ED utilization, inpatient stays (admissions and number of days), jail bookings and days spent in jail.	☒Housing services and supports ☐ Permanent supportive housing ☐ Other (write in; for example, transitional housing, emergency shelter, affordable housing):	☐ Neighborhood and built environment ☒ Economic stability ☐ Education ☐ Social and community health	Focus population is only those who are currently experiencing homelessness.
6	Mobile Crisis Intervention Services (MCIS) Startup	The goal of MCIS is to provide a community-based alternative to individuals experiencing a behavioral health crisis that does not include law enforcement. MCIS are provided in the community at times and locations that are convenient to the individual and their family. Services and supports are provided by staff trained in crisis response, in a trauma-informed manner. Individuals can receive the services and supports that they need in a timely manner. MCIS is focused on early intervention and crisis de-escalation, with a focus on diverting unnecessary trips to the emergency department, hospitalizations, child welfare involvement, juvenile justice, or arrests, and providing services and supports to the individual in the least restrictive environment necessary. Members will be connected to supports for SDOH needs will include connections to housing / shelter; food/nutrition assistance; services related to climate emergencies. Goals of the project funding for startup are to launch mobile crisis services in Lane County with an initial pilot period to assess long-term program functions to meet specific community needs.	☒Housing services and supports ☐ Permanent supportive housing ☐ Other (write in; for example, transitional housing, emergency shelter, affordable housing):	☐ Neighborhood and built environment ☐ Economic stability ☐ Education ☒ Social and community health	All members in Lane County who are adults in need of mobile response services, including Eugene/Springfield and key rural areas such as Veneta, South Lane, Oakridge, Junction City, and McKenzie Bridge/Blue River areas.

7	Perinatal to age 5 Resource Navigation Support System (Pollywog system)	The program, which is replicating the Pollywog system, includes closed loop perinatal to age five system including connecting participants to services such as pregnancy support, childbirth education, lactation support, parenting education, early learning, and social emotional health supports. Well-trained staff support navigation and connection to services utilizing Unite Us. In the first year, process measures are to hire program staff; build an updated website; launch Brightbytext; update Early Childhood Hub contracts to align with program expectations. Outcome measures are an increased enrollment in parenting education classes by 10%; serve 400 households with resource navigation/referrals; collect qualitative feedback from families.	☐ Housing services and supports ☐ Permanent supportive housing ☐ Other (write in; for example, transitional housing, emergency shelter, affordable housing):	☐ Neighborhood and built environment ☐ Economic stability ☒ Education ☒ Social and community health	Parents who are in the perinatal stage and parents with children up to age 5.
8	Professionalization of Health Care Interpreters (HCIs) in Oregon	Through the professional development of health care interpreters (HCIs) and the recruitment, training, and credentialing of new HCIs in high-demand languages, Trillium Community Health Plan, in partnership with the Oregon Health Care Interpreters Association (OHCIA), plans to address the language access crisis and health disparities in Oregon. Our goal is to increase patient safety and improve health care outcomes for individuals with limited English proficiency (LEP). The training is 60 hours and will train 30 students.	☐ Housing services and supports ☐ Permanent supportive housing ☐ Other (write in; for example, transitional housing, emergency shelter, affordable housing):	☐ Neighborhood and built environment ☒ Economic stability ☒ Education ☒ Social and community health	Members with language needs.
9	Initiative for Accelerated Nursing	This is a full-time, onsite, 12-month intensive degree program with full Commission on Collegiate Nursing Education accreditation. The school has built an expansive network of clinical partners for applied educational opportunities, such as Everyone Village, White Bird Clinic, and Trillium Children's Farm Home. These organizations include emergency shelter and healthcare for the unhoused and youth with behavioral health conditions who	☐ Housing services and supports ☐ Permanent supportive housing ☐ Other (write in; for example, transitional housing, emergency shelter, affordable housing):	☐ Neighborhood and built environment ☒ Economic stability ☒ Education ☐ Social and community health	Funding will serve enrolled nursing students, who will have a direct pathway to employment at Peace Health. Patients at

		need longer term crisis supports. These partnerships demonstrate the commitment to serving diverse populations. Nursing students will rotate through with these community partners to give the students experience working with at-risk populations. The school is focused on ensuring safe, affirming, and inclusive spaces for a diverse population of student nurses. The program produces up to 64 workforce-ready nurses a year. Completion of the new Primary Classroom is a main objective of the project. So far, the school has graduated three cohorts of students and two cohorts are currently enrolled. Forty (40) have graduated, and thirty-nine (39) are currently in Cohorts 4 or 5. In total, they have 79 students who have either graduated or are currently enrolled and projected to graduate by December 2024. Across all students enrolled throughout the life of the program, 21% identify as male, 79% identify as female, and 30% of students self-identify as non-white, white/Hispanic, Latino, or mixed race/ethnicity (significantly higher than the overall population in Lane County which is nearly 89% white). Finally, nearly 20% of students overall have self-reported as first-generation college students. The program currently boasts a 100% RN-NCLEX exam passing rate (first-time) compared to the national average of 81%.			Peace Health would be served by any nursing students hired.

CHP/statewide priorities

3. **Which specific priorities, topics or domains within your CCO's most recent shared community health improvement plan does this SHARE spending plan address? List single CHP topics in bullets and *briefly* describe how your SHARE spending plan aligns with your CCO's shared community health improvement plan.**

1. Ensure incomes are sufficient to meet basic costs of living (i.e., housing, childcare, food, transportation, etc.)
    1. Two projects have key elements related to this CHP priority, which are the Bushnell University Initiative for Accelerated Nursing and Oregon Health Care Interpreters Association's Professionalization of HCIs in Oregon through their focus on education which aim to lead to adequate income through employment.
2. Establish community conditions that support behavioral health and physical well-being.
    1. The projects with FOOD for Lane County, St. Vincent DePaul, Equitable Social Solutions, Lane County, and United Way Early Learning Hub support behavioral health and/or physical well-being as core project components.
3. Address current historical injustices that produce disparities.
    1. FOOD for Lane County addresses this element through the populations they serve; Oregon Health Care Interpreters Association's Professionalization of HCIs in Oregon addresses this element through the individuals they recruit for their training. Lane County MCIS and FUSE both aim to reduce jail bookings by upstream and early interventions. The project with Drawbridge Innovations helps support the work around HRSN, which is rooted in health equity.

4. **Briefly describe how your SHARE Initiative spending plan addresses the statewide priority of housing-related services and supports, including supported housing, and helps people find and maintain stable housing.** In the description, please reference the specific housing projects using the project numbers from the table above (question 2).
There are five projects that address the statewide priority of housing. These are projects 2, 3, 4, and 5. Project 2 increases capacity for emergency shelter; Project 3 is designed to build structure around the HRSN Housing benefit, which includes housing supports to obtain and maintain housing stability. Project 4 provides housing supports and support services to those members who do not quality for HRSN. Project 5 provides services and supports to place participants in supportive housing to help minimize participants' utilization of crisis services. Project 6 connects members to supports, including housing and shelter.

SDOH-E partners and agreements

5. Complete the table below for each funded SDOH-E partner. Duplicate the row below for each partner included in your spending plan.
    A) Identify each SDOH-E partner that will receive a portion of SHARE Initiative funding.
    B) Identify the total SHARE budget (dollar amount) being allocated to the partner.
    C) Briefly describe how the partner will be using the SHARE funds.
    Note: For each partner, your CCO must have a partner agreement in place that meets requirements in guidance. You don't need to submit the agreements to OHA.

Project # (match above)	Partner name	SHARE budget to partner ($)	Partner agreement	Describe the specific items, activities or services being funded with SHARE
1	FOOD for Lane County	$280,000	☒ Yes ☐ No	Trillium Produce Plus: purchase of fresh produce. New in 2024 will be to develop two rural sites that will distribute fresh produce and other food items to anyone in the community who is food insecure. Trillium Veggie Rx: purchase of fresh fruits and vegetables for members enrolled in Start Smart for

				Baby, who are not HRSN eligible.
2	St Vincent DePaul	$536,656	☒ Yes ☐ No	Families Annex Kitchen: capital improvements to the plumbing and a kitchen remodel. First Place Day Care: capital improvements and ADA accessibility modifications, playground facilities. Pallet Shelter: operation costs for pallet shelter/Conestoga huts that are at the Annex.
3	Drawbridge Innovations, LLC	$35,000	☒ Yes ☐ No	HRSN Housing Implementation Process Mapping: Staffing costs to complete phases in Discovery and Preparation, Stakeholder Workshops, Vision Mapping
4	Equitable Social Solutions	$264,000	☒ Yes ☐ No	Houseless Diversion and Rapid Rehousing for Non-HRSN Eligible Members: funding for staff that will be working with families to connect to housing supports; costs directly related to housing supports such as utilities and rent payments.
5	Lane County	$100,000	☒ Yes ☐ No	FUSE Program: FTE for personnel, materials & services for client assistance.
6	Lane County	$255,000	☒ Yes ☐ No	Mobile Crisis Intervention Services (MCIS) startup costs: 2 vans, computers & phones, project manager FTE, public information campaign.
7	United Way Early Learning Hub	$355,727	☒ Yes ☐ No	Perinatal to age 5 Resource Navigation Support System (Pollywog system): Bi-lingual/bi-cultural resource navigators, system development manager, technology, marketing manager/blog writer/outreach and engagement, website redesign, BrightbyText, admin/supervision.
8	Oregon Health Care Interpreters Association	$72,522	☒ Yes ☐ No	Professionalization of Health Care Interpreters in Oregon: Over three years, funds will pay for staff to support health care interpreter recruitment, training, and credentialing of new HCIs in high-demand languages. Funding will pay for credentialing expenses, CEUs, a stipend (e.g. to cover childcare, time off work, etc.); expenses related to reporting on program; expenses related to outreach and marketing for the training to recruit individuals who speak languages of limited diffusion.
9	Bushnell University	$500,000	☒ Yes ☐ No	Initiative for Accelerated Nursing: Capital expenses for a new Primary Classroom at the Center for Accelerated Nursing. This will be a space for student nurses for a significant part of their training time.

6. **Are any of your partner agreements a subcontract as defined in CCO contract?** ☐ Yes ☒ No
   If yes, which ones?

Partner selection and community advisory council (CAC role

7. **Describe the process for identifying and selecting the SDOH-E partners for SHARE Initiative projects.**

A. Below are some examples of CAC roles in SHARE. Check all boxes that apply.

☒ CAC determined SHARE priority areas.
☐ CAC created or approved the overall SHARE decision-making process.
☐ CAC developed a scoring rubric for reviewing SHARE proposals.
☐ CAC members recommended organizations to fund using SHARE dollars.
☒ CAC members reviewed SHARE proposals and made recommendations to CCO leadership.
☒ CAC made final SHARE project funding decisions.
☒ CAC will have a role in ongoing monitoring of SHARE projects.

B. **Briefly describe what steps were taken to identify and select partners and who was involved (for example, CCO leadership, CCO staff, committee, advisory group, CAC). Be sure to include your CAC's designated role in SHARE Initiative spending decisions.** (If applicable, also describe the ongoing engagement and feedback loop with the CAC as it relates to SDOH-E spending.)

Potential SHARE partners or staff presented individual projects to CAC members to review project components and receive feedback and approval of spending decisions. CAC feedback was then shared with the Executive Leadership Team. Ongoing, SHARE partners will return to the CAC to present on project progress as a part of the monitoring and evaluation plan. As we incorporate learning in our process each year for continuous improvement, one element we are adding to the next SHARE year (2025) is using polling results from the CAC to determine SHARE priority areas. We have already polled the CAC to receive input on priority areas for 2025.

Section 3: Additional details

8. **If the project or initiative requires data sharing, attach a proposed or final data-sharing agreement that details the obligation for the SDOH-E partner to comply with HIPAA, HITECH and other applicable laws regarding privacy and security of personally identifiable information and electronic health records and hard copies thereof. Does the project require data sharing?**

☒ Yes ☐ No

9. **(*Optional*) CCOs may choose to include an evaluation plan. If so, describe or attach the evaluation plan for the SHARE spending plan portfolio or for each project, including expected outcomes; the projected number of your CCO's members, OHP members, and other community members served; and how the impact will be measured.**

Click here to enter text.

CENTENE® Corporation

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("**BAA**") is between Centene Corporation, a Delaware corporation ("**Covered Entity**"), and _____, a _____ ("**Business Associate**"; individually with Covered Entity a "**Party**" and together the "**Parties**") and is effective _____. Capitalized terms not otherwise defined in this BAA have the meanings assigned to such terms in Section 1.

1. Covered Entity and/or one or more of its Affiliates desire to obtain services from Business Associate that will result in the Use of Covered Entity's (or its Affiliate's) PHI pursuant to one or more contracts between Business Associate, on one hand, and Covered Entity and/or any of its Affiliates, on the other hand, in effect on or after the effective date of this BAA (each contract, a "**Primary Agreement**"); and

2. Covered Entity and Business Associate desire and intend that this BAA govern the Use of all PHI under a Primary Agreement and all other Use of PHI by Business Associate for or on behalf of Covered Entity or Covered Entity's Affiliates.

The Parties agree as follows:

Section 1. Definitions.

The following terms (capitalized or not and including grammatical variants, such as "disclose" vs. "disclosure") in this BAA have the meaning set forth in the HIPAA Authorities, including Breach, Data Aggregation, Designated Record Set, Disclosure, Discover, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use. Business Associate is a "business associate" as defined at 45 CFR 160.103. Covered Entity is a "covered entity" as defined at 45 CFR 160.103.

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

"ePHI" means Electronic Protected Health Information.

"HIPAA Authorities" means 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 Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164, as amended.

"Incident" means (i) any successful Security Incident, (ii) Breach of Unsecured Protected Health Information, or (iii) any loss, destruction, alteration or other event in which PHI cannot be accounted for. Unless otherwise required by applicable laws, successful Security Incidents do not include pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of

CENTENE CORPORATION 7700 Forsyth Boulevard, St. Louis, MO 63105 | (314) 725-4477

service and any combination of the above, so long as no such incident results in or is related to unauthorized access, Use or Disclosure of PHI.

"Protected Health Information" or "PHI" collectively refers to Protected Health Information as defined in 45 C.F.R. §160.103.

Section 2. Interpretation of Provisions of this BAA; Application of Agreement.

2.1 If there is an inconsistency between this BAA and the mandatory terms of the HIPAA Authorities, the HIPAA Authorities will prevail. If there is a conflict between this BAA and a Primary Agreement, this BAA controls, including with respect to any Primary Agreement executed after the effective date of this BAA. Any ambiguity in this BAA will be resolved in favor of a meaning that permits Covered Entity and Business Associate to comply with the HIPAA Authorities and with Covered Entity's contract obligations to a government entity. A reference in this BAA to a section in the HIPAA Authorities means the section in effect or as amended. Titles or headings are used in this BAA for reference only and do not have any effect on the interpretation of this BAA. A reference to Business Associate will be interpreted to include its Affiliate if the Business Associate Affiliate is a party to the applicable Primary Agreement.

2.2 This BAA governs the Use of all PHI that exists or arises in connection with a Primary Agreement between the Covered Entity or its Affiliates, on the one hand, and Business Associate, on the other hand. Each Party 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 BAA for the benefit of itself and, with respect to Covered Entity, its Affiliates; (iii) this BAA is a legal and valid obligation binding upon it; (iv) Business Associate will cause all of its Affiliates that Use PHI pursuant to a Primary Agreement to comply with Business Associate's obligations under this BAA and will cause such Affiliates to execute a Business Associate Agreement that contains provisions materially similar to this BAA; and (v) its execution, delivery and performance of this BAA does not conflict with any agreement, instrument, obligation or understanding to which it or any of its Affiliates are bound. Business Associate will comply with the terms of Exhibit A – Privacy and Security Addendum.

Section 3. Permitted Uses and Disclosures.

Except as otherwise limited in this BAA, Business Associate may Use or Disclose PHI only as necessary to perform its obligations under each Primary Agreement, as long as 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. If the Business Associate is permitted to de-identify PHI in a Primary Agreement, Business Associate must de-identify PHI in accordance with 45 C.F.R. § 164.514 and not Use de-identified PHI except as expressly provided in the applicable Primary Agreement. Business Associate must ensure that its Affiliates Use PHI in accordance with this BAA and will be responsible for such Use. In addition, Business Associate may Use PHI:

3.1 To provide Data Aggregation services to Covered Entity as permitted by 42 CFR § 164.504(e)(2)(i)(B); and

3.2 For the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, except that Use or Disclosure of PHI under this section is permissible only if (a) it is Required By Law, or (b) Business Associate has obtained 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.

Section 4. Obligations of Business Associate.

Business Associate must:

4.1 Not Use or further Disclose PHI other than as permitted by this BAA or as Required by Law;

4.2 Comply with the requirements of the Privacy Rule that apply to the Covered Entity to the extent Business Associate is carrying out one or more of the Covered Entity's obligations under the Privacy Rule;

4.3 Implement and maintain reasonable and appropriate administrative, physical and technical safeguards to ensure appropriate Use or Disclosure of PHI as provided for by this agreement, each Primary Agreement and limit incidental Uses or Disclosures of PHI;

4.4 With respect to an Incident:

(a) Notify Covered Entity in writing at **privacy@centene.com** as soon as reasonably practicable, but in no event longer than 24 hours, after discovery of any Incident, notwithstanding any provision to the contrary in Section 8.10;

(b) Take prompt, reasonable steps to (a) 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 BAA or the HIPAA Authorities and (b) prevent the recurrence of any Incident, including any action required by applicable federal and state laws and regulations;

(c) Maintain the capability to identify the covered entity to which information involved in an Incident relates if Business Associate creates, receives, maintains, or transmits PHI on behalf of other covered entities in addition to Covered Entity;

(d) Deliver to Covered Entity within 14 calendar days after discovery of an Incident a written corrective action plan ("**CAP**") describing, at minimum, the measures Business Associate has taken and intends to take to halt or contain the Incident and mitigate the effects of the Incident as provided in Section 4.5, and, if the CAP is approved by Covered Entity, promptly and fully implement any remaining requirements of the CAP;

(e) Deliver to Covered Entity as soon as reasonably practicable, but no more than 14 calendar days following discovery of an Incident, a written report that includes: (a) a description of the circumstances under which the Incident occurred; (b) the date of the Incident and the date that the Incident was discovered; (c) a description of the types of PHI involved in the Incident; (d) identification of each Individual whose PHI is known or reasonably believed by the Business Associate to have been affected; and (e) any recommendations that the Business Associate may have regarding the steps that Individuals may take to protect themselves from harm;

(f) Fully cooperate, coordinate with, and assist Covered Entity in gathering information necessary to notify the affected individuals and government agencies following an Incident to ensure that any notices sent in connection with the Incident are sent without unreasonable delay, and in no case more than 60 calendar days after discovery of the Incident, and perform such notifications if so required by Covered Entity in its sole discretion;

(g) Be solely responsible for all costs and expenses incurred as a result of an Incident related to a Primary Agreement or other Use or Disclosure by Business Associate, including costs associated with mitigation of the Incident and preparation and delivery of notices to affected individuals and government agencies;

(h) Cooperate with any investigation (and/or risk assessment) of an Incident conducted by or on behalf of Covered Entity in connection with an Incident and make itself and its applicable subcontractors and agents available to Covered Entity to testify as witnesses, or otherwise, in the event of an Incident;

4.5 With respect to any Subcontractor:

(a) Ensure that, before a Subcontractor (including any Affiliate that is a Subcontractor) creates, receives, maintains, or transmits PHI on behalf of Business Associate, the Subcontractor enters into a written agreement with the Business Associate (the "**Subcontractor Agreement**") obligating the Subcontractor: (i) to comply with the same HIPAA Authorities that apply to Business Associate under the Primary Agreement; and (ii) to comply with the same restrictions and conditions that apply to Business Associate through this BAA with respect to such PHI;

(b) Upon Business Associate's knowledge of a material breach of a Subcontractor Agreement provision related to PHI by Subcontractor or of an act or omission of Subcontractor that would be a breach of this BAA if performed by Business Associate, (I) immediately notify Covered Entity in writing and (II) at Business Associate's option (unless otherwise directed by Covered Entity): (i) terminate the Subcontractor Agreement if Subcontractor does not cure the material breach within the cure period for material breach specified in the Primary Agreement after Business Associate notifies Subcontractor of the material breach, or if no cure period is identified in the Primary Agreement, as specified by Covered Entity; or (ii) immediately terminate the Subcontractor Agreement if Business Associate (or Covered Entity) deems cure by the Subcontractor not to be possible; and

(c) Upon request, provide Covered Entity with a list of any and all of its Subcontractors that create, receive, maintain or transmit PHI on behalf of Business Associate in connection with Business Associate's obligations under the applicable Primary Agreement within 30 calendar days.

4.6 If Business Associate maintains any Designated Record Set:

(a) At the request of Covered Entity and within 15 calendar days after such request, make available PHI in a Designated Record Set to Covered Entity or, as directed by Covered Entity, to an Individual, in a manner acceptable to Covered Entity and compliant with 45 CFR §164.524 and/or other applicable provisions of the HIPAA Authorities;

(b) Make any amendment(s) to PHI in a Designated Record Set to which the Covered Entity has agreed pursuant to 45 CFR §164.526 within 15 calendar days of following a request by Covered Entity, or as

directed by Covered Entity, following a request of an Individual, and in a reasonable manner designated by Covered Entity, and otherwise assist Covered Entity in complying with Covered Entity's obligations under 45 CFR §164.526;

(c) Ensure that PHI in a Designated Record Set is available in an electronic format, in accordance with 45 C.F.R. § 164.524, as long as the request is made in accordance with HIPAA;

4.7 Make its internal practices, books and records available to the Secretary or to the Covered Entity for purposes of determining Business Associate's compliance with the HIPAA Authorities, in a time and manner designated by Covered Entity or the Secretary, as applicable. Covered Entity will provide a reasonable notice period for performing any such review or request for access to documentation and will not perform any such review or request for access to documentation more than once in a calendar year except (a) following, and in response to, an Incident, (b) Covered Entity reasonably believes that Business Associate has breached the obligations of this BAA, or (c) as required by law or as requested by a government agency. Business Associate will perform activities under this section during Business Associate's normal business hours on a non-interfering basis and subject to Business Associate's customary policies and procedures governing facility and infrastructure access (except to the extent such policies and procedures would bar Business Associate's performance under this section);

4.8 Document all Disclosures of PHI (other than those expressly exempted from documentation requirements under the HIPAA Authorities) 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;

4.9 Provide an accounting of Disclosures of PHI to Covered Entity or an Individual within 15 calendar 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;

4.10 Retain documentation of Disclosures of PHI for a minimum of 6 years, unless otherwise provided under the HIPAA Authorities or the Primary Agreement;

4.11 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 BAA and the Primary Agreement, including with respect to Uses and Disclosures by and among members of Business Associate's workforce as well as by or to third parties;

4.12 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 BAA 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; and

4.13 Not sell Protected Health Information without authorization pursuant to 45 C.F.R. § 164.502

(a)(5)(ii).

Section 5. Obligations of Covered Entity.

Covered Entity will:

5.1 Notify Business Associate of any limitation in Covered Entity's notice of privacy practices, to the extent that such limitation may affect Business Associate's Use or Disclosure of PHI;

5.2 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;

5.3 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; and

5.4 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, except as necessary for the Data Aggregation Services or management and administrative activities of the Business Associate as allowed in this BAA.

Section 6. Indemnification.

Business Associate will defend, indemnify and hold harmless Covered Entity, its Affiliates and their respective directors, officers and employees from and against all claims, causes of action, damages and expenses (including reasonable attorneys' fees) arising out of or relating to any Incident or breach of this BAA by Business Associate and its Subcontractors and Affiliates. The exclusions and limits of liability, if any, provided in the Primary Agreement(s) do not apply to damages arising from a breach of the foregoing obligations.

Section 7. Term and Termination.

7.1 **Term.** This BAA will be effective beginning on the effective date of this BAA and will remain in effect with respect to each Primary Agreement during the term of the Primary Agreement, unless earlier terminated as provided in this BAA.

7.2 **Termination with Cause.** Upon Covered Entity's knowledge of a material breach of this BAA by Business Associate or its Subcontractors, Covered Entity may, at its option: (a) provide an opportunity for Business Associate to cure the breach or end the violation and terminate this BAA and any applicable Primary Agreement if Business Associate does not cure the breach or end the violation within the cure period identified in the Primary Agreement, or if no cure period is identified in the Primary Agreement, as specified by Covered Entity; or (b) immediately terminate this BAA if Business Associate has breached a material term of this BAA and Covered Entity deems cure by Business Associate not to be possible.

7.3 **Effect of Termination.**

(a) Except as provided in Section 7.3(b), upon termination of this BAA for any reason, Business Associate will promptly return or destroy (at Covered Entity's election and in a manner compliant with Section 4.4 of this BAA), and is not permitted to retain copies of, all PHI and, if applicable, de-identified PHI in the possession of Business Associate or its Subcontractors. Business Associate will provide written certification of destruction of data as required in this section that is acceptable to Covered Entity.

(b) If Business Associate determines that returning or destroying the PHI is infeasible, Business Associate must provide to Covered Entity prompt written notification of the conditions that make return or destruction infeasible. Upon Covered Entity's written approval, which will not be unreasonably withheld, Business Associate may retain the PHI ("**Retained PHI**"), but (i) the terms of this BAA will apply to any Retained PHI for as long as Business Associate retains the PHI, even if the BAA has been terminated, and (ii) Business Associate will limit further Use and Disclosure of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

Section 8. Miscellaneous

8.1 Response to Subpoena. Business Associate may Disclose PHI to the extent required by court order, subpoena or other compulsory legal process, but only if, prior to making any Disclosure thereunder, Business Associate provides Covered Entity at least 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.

8.2 Compliance with Law. Business Associate will comply with all applicable laws, including the 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 BAA pursuant to the HIPAA Authorities, are incorporated into this BAA by this reference.

8.3 Assignment; Waiver. This BAA will bind and inure to the benefit of the respective legal successors of the Parties. Neither this BAA 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 BAA creates no independent rights in any third party or makes any third party a beneficiary hereof. No failure or delay by either Party in exercising its rights under this BAA will operate as a waiver of such rights, or of any prior, concurrent, or subsequent breach.

8.4 Property Rights. All PHI is and will 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 BAA.

8.5 Right to Cure. Business Associate agrees that if Business Associate fails to cure a breach of this BAA pursuant to this BAA, Covered Entity has the right, but not the obligation, to cure the same. Business Associate is solely responsible for expenses, costs or fines reasonably incurred in connection with Covered Entity's cure of Business Associate's breach of its obligations under this BAA.

8.6 Injunctive Relief. Business Associate agrees that breach of the terms and conditions of this BAA will 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 BAA, 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.

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

8.8 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 BAA 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 BAA will 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.

8.9 Governing Law. This BAA will be governed by and construed in accordance with the laws of the State of Missouri to the extent that the HIPAA Authorities do not preempt the same.

8.10 Notice. Any notice required or permitted to be given by either Party under this BAA (except those required pursuant to Section 4.7) will be sufficient and effective if (a) in writing and hand delivered (including delivery by courier), or (b) delivered by a national overnight parcel carrier, in each case to the applicable address set forth below the receiving Party's signature below. Without limiting the previous sentence, the Party providing notice must provide a copy of any notice under this section via email with return receipt requested to the email address in the signature block below or, if no email address is provided, to the primary business owner of the Party receiving notice.

8.11 Independent Contractors. For purposes of this BAA, 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 BAA will establish or be deemed or construed to establish any partnership, agency, employment agreement or joint venture between the parties.

8.12 Authority. Each Party to this BAA warrants that it has full power and authority to enter into this BAA, and the person signing this BAA on behalf of either Party warrants that he/she has been duly authorized and empowered to enter into this BAA.

Signatures on the following page

Acknowledged and agreed:

COVERED ENTITY

By:_____
Name:_____
Title:_____
Date:_____

Notice Address:

7700 Forsyth Blvd
St. Louis, MO 63105
Attention: Privacy Department
With a copy to: Legal Department
Phone: (314) 320-2661
Email: privacy@centene.com

BUSINESS ASSOCIATE

By:_____
Name:_____
Title:_____
Date:_____

Notice Address:

_____
_____
_____
Attention: _____
Phone: _____
Email: _____

Exhibit A –Security and Privacy Addendum

Security Governance, Risk Management 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) A privacy officer must be assigned.

2. Security Training & Awareness

    a) An on-going and documented privacy and security awareness program must be established.

    b) Users must be aware of the company's privacy and security policies and the requirements to protect the information.

    c) Privacy and security awareness information must be distributed to all users on a defined periodic basis, no less than once per year.

    d) Mandatory privacy and security training must be delivered to, managed, and validated for all users at least once per year.

3. Privacy and Security Assessments

    a) An accurate and thorough assessment of the risks to the confidentiality, integrity, and availability of confidential information, including PHI and ePHI must be conducted at least once per year. Identified risks must be formally documented and managed through the risk management function and/or program.

4. Policies, Standards, and Procedure Management

    a) The following documented functions/ and/or programs must exist and be supported by executive management:
        i. risk management function and/or program
        ii. information security function and/or program
        iii. privacy function and/or program supported

    b) The risk management function and/or program must establish a repeatable process to assess gaps or deviations in the security posture for risk to the organization. Risk ownership and treatment must be identified by an appropriate level of management.

c) 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.

d) The privacy function/program must establish confidentiality policies that are maintained and updated as needed.

5. Issue and Corrective Action Management

a) Controls must be implemented to reduce risks and vulnerabilities to a reasonable and appropriate level, within the risk appetite.

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.

6. 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.

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 approved subcontracts.

2. Contract & Service Initiation

a) Subcontracted third parties with controls deviating from security requirements must be assessed for risk and have management action plans in place to mitigate to an acceptable risk level.

b) All subcontracts must contain all privacy and security requirements and protections as set forth in this Security Addendum.

c) Information containing PHI or ePHI must only be disclosed to third parties when a Business Associate Agreement 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 outsourced 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 supporting this contract must be identified and documented.

    b) Agents, subcontractors, and outsourced services identified as providing critical services, or 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 must never 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 terminated users,
        - 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 with descriptions of 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 must not be scripted into the application.

f) System IDs must not be accessible 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, must have system access controls to prevent unauthorized disclosure or modification.

b) Single sign on technologies must be 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 must be subject to the same Identity Management requirements as Company personnel.

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, must be 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 with FIPS 140-2 compliant encryption protocols during storage on all devices including handhelds, laptops, workstations, and removable media.

    b) Information containing PHI and ePHI must be encrypted with FIPS 140-2 compliant encryption protocols during storage on servers.

    c) Confidential information, including PHI and ePHI, must be encrypted with FIPS 140-2 compliant encryption protocols during transmission over public or untrusted networks, including wireless or email transmissions.

    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 for the removal or movement of confidential information, including PHI and ePHI to unsecured systems or media must exist.

    b) Confidential information, including PHI and ePHI, stored on removable media must be secured with access restricted 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 for the removal or destruction of confidential information, including PHI and ePHI must exist. When appropriate, confidential

information, including PHI and ePHI, must be purged or destroyed using a NIST 800-88 approved process when no longer needed.

Secure Development Lifecycle

1. Security and Risk Requirements

    a) The System Development Life Cycle must include a documented process 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.

    b) Security controls must be considered throughout the System Development Life Cycle.

2. Security Design & Architecture

    a) Security controls must be designed to eliminate single points of failure.

    b) Systems must be 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 must be designed to ensure users can access only information they have an authorized business need for.

    b) Access must be controlled by a common access methodology or single sign on wherever feasible.

4. Secure Coding Guidelines

    a) Secure coding principles and practices must be 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 must be used for code review.

7. Roll-out and Go-live Management

    a) To retain separation of duties, staff other than developers must be responsible for moving systems or applications into the production environment.

    b) All non-standard access paths must be removed prior to being moved into production.

8. Application Security Administration

    a) Development staff must receive management approval to access production systems.

    b) Technical staff must not have access to production data, programs, or applications unless such access is required to perform their jobs.

Infrastructure, Operations and Network Security

1. Antivirus (AV) & Malware protection

    a) Documented policies and procedures for guarding against, detecting, and reporting malicious software must exist.

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) Documented policies and procedures to prevent unauthorized/unsecured devices from accessing the network must exist.

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) Documented policies and procedures to prevent confidential information, including PHI and ePHI, from being transmitted to unauthorized recipients or stored in unauthorized locations must exist.

6. Remote Access Controls

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

7. Security Monitoring

    a) Documented policies and procedures to monitor networks, systems, and applications for potential security events must exist.

    b) A documented process to respond to potential security events on a 24x7x365 basis must exist.

    c) All significant computer security relevant events must be securely logged, and the logs must be periodically reviewed.

    d) Computer systems handling confidential information, including PHI and ePHI, must securely log all significant computer security relevant events, including the following:

        i. unauthorized attempts to enter the system,
        ii. unauthorized attempts to access protected information or resources,
        iii. all attempts to issue restricted commands,
        iv. security activities,
        v. special privileged user activities and
        vi. violation activities.

    e) All logs of computer security relevant events must be traceable to specific individuals wherever possible.

8. Wireless Security Controls

    a) Documented policies and procedures to prevent unauthorized wireless access to production systems must exist.

9. Database Security

    a) Documented policies and procedures to prevent unauthorized updates to databases must exist.

    b) All database access must be traceable to specific individuals.

10. Network Device Security

    a) All network devices supporting business critical systems must have physical and logical access controls.

    b) All network devices supporting business critical systems must 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 to periodically verify security configuration settings must exist.

    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 or less of inactivity.

2. Patch Management

    a) A documented patch management process must exist and be enforced.

    b) Security patches, service packs, & hot fixes must be promptly applied for all systems that store, process, manage, or control access to sensitive data, including PHI and ePHI.

3. Vulnerability Management

    a) Documented processes and procedures to identify, quantify, prioritize, track, and remediate vulnerabilities must exist.

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 to evaluate current capacity against projected requirements must exist.

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.

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

c) 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.

d) Production code and systems must not allow undocumented changes or updates.

9. Asset and Configuration Management

a) Documented network diagrams must exist.

b) An auditable and documented inventory of information technology assets must exist in case of loss or theft.

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.

b) Business Associate must conduct a Business Impact Analysts (BIA) at a minimum of every two (2) years. The BIA must identify critical business processes, assets, and locations. The results of the BIA must be used to identify potential business disruptions, create mitigation and remediation plans, and enhance the resiliency of the organization.

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 incremental 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.

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) Suspected cyber security incidents with a potential impact on Centene data and/or systems must be reported to Centene's Vice President of Cybersecurity within 24 hours. Examples include:

        a. Compromised email accounts that may affect Centene
        b. Compromised systems that have a trusted link to Centene networks
        c. Malware infections on systems used for Centene business

    c) Centene must have full control of messaging to media in the event of a potential security incident that affects Centene

    d) The Data Center facility must be equipped and maintained with fire detection/suppression, surge and brownout, air conditioning, and other computing

environment protection systems necessary to assure continued service for critical computer systems.

e) Policies and procedures must be in place to document repairs and modifications to physical components related to security (hardware, walls, doors and locks, etc.) of facilities where PHI and ePHI are stored.

f) All hardware and electronic media containing PHI and ePHI must be identified and tracked during movement.

g) 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.

Data Sharing Agreement

This contract is made and entered into by and between Centene Management Company, LLC, a Wisconsin limited liability company ("**Centene**"), and Counterparty Legal Name, Counterparty Entity Type (such as "a Delaware corporation") ("**Company**"), and is effective when signed by both parties.

A. %% Centene and Company are each business associates of the State of _____ (the "State"); and

B. The State has instructed Centene to provide certain Information (defined below) to Company in connection with _____ (the "**Purpose**"); and // These opening recitals must be tailored to the specifics of why and how the information is being transferred. %

C. The parties desire to identify their respective rights and obligations with respect to the Information; and

D. The parties, therefore, enter into this contract intending to protect the integrity and confidentiality of the Information and comply with applicable legal and regulatory requirements related to the Information.

The parties agree as follows:

1. Definitions

1.1 "**Information**" means PHI (defined below) and other nonpublic information provided by Centene to Company.

1.2 "**PHI**" means protected health information as defined in the Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") and regulations promulgated thereunder, including electronic PHI (whether or not encrypted) and PHI that has been deidentified or aggregated.

1.3 Other capitalized terms used and not defined in this contract have the same meaning as set forth in 45 CFR Part 160-164.

2. Scope and purpose

2.1 This contract sets forth the terms and conditions pursuant to which Company will Use and Disclose any Information provided by Centene or created by Company on Centene's behalf.

2.2 Centene will provide Information %% as instructed by the State // USEIF: transfer is required by a government entity %% in accordance with the Purpose. This contract does not relate to any other sharing of materials or information, and this contract does not require Centene to share any materials or information for any reason other than the Purpose.

2.3 If required by applicable Law, the parties will enter into additional agreements, such as a business associate agreement acceptable to Centene. Company will cooperate with Centene in connection with any matters arising under this contract, including disputes.

3. Restrictions on use

3.1 Company will not Use or Disclose the Information other than as permitted by this contract or by Law.

3.2 Company will use appropriate safeguards to prevent Use or Disclosure of the Information other than as provided for by this contract or by Law.

3.3 Company will report to Centene any Use or Disclosure of the Information not provided for by this contract or by Law of which it becomes aware immediately, but no later than within 24 hours after discovery of the unauthorized Use or Disclosure. As between the parties, Centene will have no financial responsibility in connection with an unauthorized Use or Disclosure of Information experienced by Company or a Company subcontractor or other agent.

3.4 Access to the Information must be limited to the minimum number of individuals necessary to achieve the Purpose.

3.5 Company will ensure that any agent, including a subcontractor, to whom it provides the Information agrees to the same restrictions and conditions that apply through this contract with respect to such information, including, if applicable, a business associate agreement that complies with HIPAA and the notification requirements in this contract.

3.6 Company will indemnify, defend and hold harmless Centene, its affiliates, and their respective trustees, officers, directors, employees and agents from and against any claim, cause of action, liability, damage, cost or expense (including, without limitation, reasonable attorney's fees and court costs) arising out of or in connection with any unauthorized or prohibited Use or Disclosure of the Information or any other breach of this contract by Company or any subcontractor, agent or person under Company's control.

4. Term and termination

4.1 This contract will remain in effect until the Purpose is accomplished unless earlier terminated.

4.2 Either party may terminate this contract for any reason upon 5 days written notice to the other party. Upon termination, Centene will cease providing Information to Company and Company will, to the extent practicable, return or destroy Information it previously received from Centene. If it is infeasible to return or destroy the Information, Company may maintain the Information so long as protections are extended to such Information, in accordance with this contract, applicable Laws and Regulations, and the requirements of the State.

5. Miscellaneous

5.1 The parties agree to take such action as is necessary to amend this contract from time to time as is necessary for the parties to comply with the requirements of applicable Laws and Regulations.

5.2 There are no intended third-party beneficiaries to this contract. Without in any way limiting the foregoing, it is the parties' specific intent that nothing contained in this contract gives rise to any right or cause of action, contractual or otherwise, in or on behalf of the individuals whose PHI is Used or Disclosed pursuant to this contract.

5.3 No provision of this contract may be waived except by a writing signed by an authorized representative of the waiving party. A waiver of any term or provision shall not be construed as a waiver of any other term or provision. This contract may not be amended except in a written agreement signed by authorized representatives of both parties.

5.4 The persons signing below have the right and authority to execute this contract and no further approvals are necessary to create a binding agreement.

5.5 This contract will be construed in accordance with and governed by the laws of the state of Missouri.

Acknowledge and agreed:

Centene Management Company, LLC	**Counterparty Legal Name**
Signature: Title:	Signature: Title:
Notice address:	*Notice address:*
7700 Forsyth Blvd. St. Louis, MO 63105 Attention: Enterprise Procurement Email: procurement-notices@centene.com	Street address (multiple lines acceptable). City., State or province ZIP or postal code Country. Attention: Name or title. Email: Notice email.