Data Sharing Agreement

This Data Sharing and License Agreement ("Agreement") is entered into by and between the State of Colorado (the "State") acting by and through the Department of Health Care Policy and Financing ("Transferring Agency"), for the use and benefit of the Transferring Agency, having an address at 1570 Grant Street, Denver, CO 80203 and [INSERT OFFICIAL NAME OF AGENCY RECEIVING DATA] ("Recipient"), whose principal office is located at [INSERT ADDRESS OF RECIPIENT]. Transferring Agency and Recipient are each individually a "Party" and together the "Parties."

Whereas, Transferring Agency is charged with the distribution of federal funding through ARPA 3.07 Wraparound Services, Including Peer Supports for Members with Complex Needs. This funding is aimed to serve a priority population of Health First Colorado (Colorado's Medicaid program) members with complex needs and a history of homelessness. To best utilize this federal funding, Transferring Agency created the Statewide Supportive Housing Expansion (SWSHE) Pilot Project ("the Pilot Project"), a grant project which connects eligible Medicaid members with a housing voucher and wraparound supportive services funding.

Whereas, Recipient is a Continuum of Care entity responsible for coordinating the delivery of housing and services for people experiencing homelessness in its service area. Specifically, a Continuum of Care (CoC) helps communities plan for and provide a full range of emergency, transitional, and permanent housing and other services to address the needs of persons experiencing homelessness. This includes managing the Homeless Management Information System (HMIS) to provide appropriate referrals, including, but not limited to, referring HMIS clients to Supportive Housing organizations.

In order to identify eligible participants for the Pilot Project, Transferring Agency entered into a Data Use Agreement (executed 8/1/2022) with Recipient. Recipient shared with Transferring Agency a list of Homeless Management Information System (HMIS) clients who have been identified as chronically homeless and/or prioritized for a Permanent Supportive Housing (PSH) intervention through the Coordinated Entry system ("Active By Name List"). The reason each individual is on this list is because they gave Recipient permission to seek and coordinate housing and supportive service resources on their behalf. Upon receiving this data, Transferring Agency further prioritized the list based on additional Medicaid Management Information System (MMIS) data and created the 'SWSHE-eligible Coordinated Entry List'. This list is a modification of the Active By Name List which only includes individuals eligible to participate in the Pilot Project.

Whereas, Transferring Agency wishes to disclose to Recipient the 'SWSHE-eligible Coordinated Entry List' so that Recipient may refer eligible members to a housing voucher and supportive services. This is the mechanism by which eligible members shall be enrolled into the Pilot Project, based on availability of resources.

Whereas, in exchange for the data Recipient requested, the Recipient will refer SWSHE-eligible members to a SWSHE-contacted Supportive Housing organization (listed below in Section 3), in accordance with the terms of the ARPA grant, and as housing vouchers become available. This work will benefit Transferring Agency's eligible members who will be matched with a housing voucher and supportive services by the Supportive Housing organization. This entails enhanced care coordination and improved service delivery for this priority population.

Now, therefore, in consideration of the mutual promises contained herein, the sufficiency of which each Party hereby acknowledges as adequate, the Parties agree as follows:

1. **Defined Terms.**

a) "Anonymized Data" means Data that has been properly De-identified.

b) "Care Coordination" means the coordination of healthcare or other services that support an individual's overall health and wellbeing.

c) "CORA" means the Colorado Open Records Act, § 24-72-200.1, *et seq.*, C.R.S.

d) "Covered Entity" shall have the same meaning as the term "covered entity" at 45 C.F.R. 160.103.

e) "CJI" means all FBI CJIS-provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including, but not limited to: biometric, identity history, person, organization property (when accompanied by any PII), and case/incident history data. In addition, CJI refers to FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to, data used to make hiring decisions. The following type of data is exempt from the protection levels required for CJI: transaction control type number (e.g. ORI, NIC, FNU, etc.) when not accompanied by information that reveals CJI or PII.

f) "CJIS Addendum" means the addendum attached to this Agreement as Addendum 1.

g) "Data" means the information described in Appendix A.

h) "Data Breach" means an event resulting in an unauthorized access, use, exposure, disclosure, exfiltration, or loss of Data.

i) "De-identified" means the removal of all PII from the Data so that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. If the Data is subject to HIPAA, "De-Identified" means the removal of PII from the Data in accordance with HIPAA.

j) "Destroy" means to remove Data from Recipient's systems, paper files, records, databases, and any other media regardless of format, in accordance with the standard detailed in the OIT Security Policy.

k) "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and subsequent Amendments.

l) "Incident" means an event that results in or constitutes an imminent threat of the unauthorized access, use, loss, disclosure, modification, disruption, or destruction of communication and information resources of the State.

m) "OIT" means the Governor's Office of Information Technology.

n) "OIT Security Policies" means the security policies established by OIT to secure information held by State Agencies, which are available at: https://oit.colorado.gov/standards-policies-guides/technical-standards-policies.

o) "Protected Health Information" has the same meaning as such term is defined in HIPAA.

p) "PII" means information which can reasonably be used to identify, contact or locate an individual, either alone or in combination with other information.

2. **Sharing of Data.** Transferring Agency will share the Data described in Appendix A with Recipient one time via an encrypted email. This is a secure method agreed to by the Parties and in accordance with the OIT Security Policies.

3. **Data Use and Restrictions.** Transferring Agency hereby grants Recipient a limited, revocable right to use the Data solely for purposes of connecting eligible SWSHE participants with a housing voucher and a Supportive Housing organization (the "Purpose"). Specifically, Recipient may refer an eligible individual to the following Supportive Housing organization(s): ENTER

   a) **Disclosure to Third Parties.** Recipient shall not sell, lease, rent, loan, transfer, distribute, alter, mine or disclose the Data, including but not limited to, metadata and Anonymized Data, with any third party without the prior written consent from Transferring Agency, except the organization(s) listed above. Without limiting the generality of the preceding sentence, Recipient may not and will not use or disclose any PII for the purpose of investigating for, participating in, cooperating with, or assisting Federal Immigration Enforcement, including the enforcement of civil immigration laws, and the Illegal Immigration and Immigrant Responsibility Act, which is codified at 8 U.S.C. §§ 1325 and 1326, unless required to do so to comply with Federal or State law, or to comply with a court-issued subpoena, warrant or order.

   b) **Restrictions on Access.** Recipient shall not disclose the Data to anyone other than Recipient's personnel and contractors who have a need to know or access the Data in order to support the Purpose.

   c) **Contractors.** Recipient will not share the Data with any contractors or third parties without Transferring Agency's prior written approval, which may be received by email. Recipient agrees that any contractors or third parties that are authorized to access the Data must be subject to terms that are as restrictive as the terms contained in this Agreement.

   d) **Data Security Requirements.** Recipient agrees to secure and protect the Data against any unauthorized use or access in accordance with the most recent version of the OIT Security Policies.

   e) **Storage of Data.** Recipient agrees to: (i) use, hold, and maintain the Data in compliance with any and all applicable laws and regulations, (ii) store the Data only in facilities located within the United States, and (iii) maintain the Data in a secure environment in accordance with the OIT Security Policies.

   f) **Destruction of Data.** Upon Transferring Agency's request, or upon any termination or expiration of the Agreement, Recipient shall Destroy or return any Data in its possession, pursuant to Transferring Agency's instructions, in accordance with OIT Security Policies. Upon Transferring Agency's request, Recipient shall certify in writing that it has Destroyed the Data within thirty (30) days of Recipient's receipt of Transferring Agency's request.

   g) **Reservation of Rights.** Except for the rights explicitly granted under this Agreement, Recipient is not granted any rights in and to the Data, including, but not limited to, any Anonymized Data.

   h) **Research, Analytics and Published Materials.** To the extent the Purpose includes the need to publish materials that are based on or include the Data, Recipient may publish and share the results of such research or analytics, provided that such reports include only Anonymized Data.

The Parties may also work together to publish joint reports, as well as publish Anonymized Data on public dashboards.

i) **Linking Data to other Datasets.** Transferring Agency agrees that Recipient may include the Data with data from other sources in carrying out the Purpose. Once included, Transferring Agency agrees that the Data will be integrated into Recipient's databases. Recipient agrees that such combined datasets will treat and safeguard the data in accordance with all applicable laws.

4. **Security Incident and Data Breach.**

a) **Incident Response.** If Recipient becomes aware of an Incident, Recipient shall fully investigate and resolve the Incident and take steps to prevent developments that may result in the Incident becoming a Data Breach in accordance with all applicable privacy and security laws.

b) **Data Breach Response.** Immediately upon becoming aware of a suspected or actual Data Breach, Recipient shall: (i) notify Transferring Agency of the Data Breach in writing, (ii) start a full investigation into the Data Breach, (iii) cooperate fully with Transferring Agency's investigation of and response to the Data Breach, and (iv) use commercially reasonable efforts to prevent any further Data Breach in accordance with applicable privacy and security laws. If notification of the Data Breach is required pursuant to applicable law, Recipient shall coordinate with Transferring Agency in delivering such notifications and shall be responsible for all costs associated with such notification. In the event the Parties determine that Recipient should deliver the necessary notifications, Recipient shall obtain Transferring Agency's prior written approval of the notifications prior to distributing such notifications.

c) **Data Breach Report.** If Transferring Agency reasonably determines that a Data Breach has occurred, then Transferring Agency may request that Recipient submit a written report, and any supporting documentation, identifying (i) the nature of the Data Breach including the dates of the Data Breach, when Recipient discovered the Data Breach, and number of impacted individuals, (ii) the steps Recipient has executed to investigate the Data Breach, (iii) what Data or PII was used or disclosed, (iv) who or what was the cause of the Data Breach, (v) what Recipient has done or shall do to remediate any deleterious effect of the Data Breach, and (vi) what corrective action Recipient has taken or shall take to prevent a future Incident or Data Breach. Recipient shall deliver the report within seven (7) days of Transferring Agency's request of the report. If the Recipient learns of more information necessary for understanding the nature of the Data Breach, risk to the Data, remediation efforts, or notification requirements after submitting the report, Recipient shall update Transferring Agency without delay.

d) **Effect of Data Breach.** Transferring Agency may terminate this Agreement immediately, at its sole discretion, upon the occurrence of a Data Breach. In addition, Transferring Agency may restrict Recipient's access to the Data and require Recipient to suspend all work involving the Data, pending the investigation and successful resolution of any Data Breach.

e) **Liability for Data Breach.** Without limiting any other remedies Transferring Agency may have under law or equity, Recipient shall reimburse Transferring Agency in full for all costs, including but not limited to, payment of legal fees, audit costs, fines, and other imposed fees arising out of or relating to a Data Breach that Transferring Agency actually incurs. All responsibilities of Recipient under this Section 4 shall be completed by Recipient at Recipient's sole cost, without any right of reimbursement, set-off, payment, or remuneration of any kind from Transferring Agency.

5. **Term and Termination.**

   a) The "Term" of this Agreement shall be six (6) months from the last date of execution set forth on the signature page unless terminated sooner pursuant to the terms herein. At the end of the Term, this Agreement shall not be renewed.

   b) Transferring Agency may suspend its performance or terminate this Agreement immediately upon written notice to Recipient in the event of Recipient's breach of any of its obligations under Sections 3 or 4. In addition to any other remedies allowed by law, Transferring Agency shall have the right to require the immediate return or destruction of all Data and Anonymized Data, without opportunity to cure. It shall not constitute a breach of this Agreement for Transferring Agency to direct return or destruction of Data or Anonymized Data on a good faith belief that a breach of any of Sections 3 or 4 have occurred or could occur in the future.

6. **Indemnification.** Recipient shall indemnify, save, and hold harmless the State, its employees, agents and assignees (the "Indemnified Parties"), against any and all costs, expenses, claims, damages, liabilities, court awards and other amounts (including attorneys' fees and related costs) arising out of or related to any act or omission by Recipient, or its employees, agents, subcontractors, or assignees in connection with this Agreement, including but not limited to any breach of this Agreement by Recipient.

7. **Injunctive Relief.** Recipient acknowledges and agrees that any breach of Sections 3 or 4 could result in irreparable harm for which monetary damages are an insufficient remedy. In addition to other remedies it may have at law, including an injunctive remedy as may be allowed by law for any other breaches of this Agreement by Recipient, Recipient acknowledges and agrees that the State may seek equitable relief for any threatened or actual breaches of Sections 3 and 4 without the posting of a bond.

8. **Insurance.** Recipient shall obtain and maintain insurance as specified in this section at all times during the term of this Agreement. All insurance policies required by this Agreement shall be issued by insurance companies as approved by the State.

   a) **Cyber/Network Security and Privacy Liability.** Liability insurance covering civil, regulatory, and statutory damages, contractual damages, data breach management exposure, and any loss of income or extra expense as a result of actual or alleged breach, violation or infringement of right to privacy, consumer data protection law, confidentiality or other legal protection for personal information, as well as State Confidential Information with minimum limits as follows:

      i) $1,000,000 each occurrence; and

      ii) $1,000,000 general aggregate.

   b) For all policies, Recipient agrees:

      i) **Additional Insured**. The State will be named as an additional insured. The State may, at any time, require that Recipient provide evidence of such insurance via a Certificate from the insurer.

      ii) **Primacy of Coverage**. Coverage required of MPC and each subcontractor shall be primary over any insurance or self-insurance program carried by Recipient or the State.

iii) **Cancellation**. The above insurance policies shall include provisions preventing cancellation or non-renewal, except for cancellation based on non-payment of premiums, without at least 30 days prior written notice to Recipient and the State.

1. **Audit Rights**. Transferring Agency reserves the right, in its sole discretion and at Recipient's sole expense, to audit Recipient's performance under this Agreement to ensure compliance with the CJIS Security Policy upon thirty (30) days prior written notice to Recipient. This Audit will not occur more than once in a calendar year and may be performed by the State, or by a third party selected by the State to perform such an audit.

2. **General Provisions.**

a) **Amendment.** The Parties may only amend this Agreement in a writing signed by both Parties.

b) **Assignment.** Recipient may not transfer or assign its rights without Transferring Agency's prior, written consent. Any of Recipient's attempts at assignment or transfer without such consent shall be void. If Transferring Agency approves any assignment or transfer of Recipient's rights and obligations, this Agreement will continue to govern such rights and obligations.

c) **Counterparts.** The Parties may execute this Agreement in multiple, identical, or original counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

d) **Entire Understanding.** This Agreement, including, but not limited to, the recitals, which are incorporated into this Agreement by reference, represents the complete integration of all understandings between the Parties related to the data sharing. All prior representations and understandings related to the data sharing, oral or written, are merged into this Agreement. Prior or contemporaneous additions, deletions, or other changes to this Agreement shall not have any force or effect whatsoever, unless embodied herein.

e) **Severability.** The invalidity or unenforceability of any provision of this Agreement shall not affect the validity or enforceability of any other provision of this Agreement, which shall remain in full force and effect, provided that the Parties can continue to perform their obligations under this Agreement in accordance with the intent of this Agreement.

f) **Survival.** Sections 1, 3, 4, 6, 7, 9 and 10 of this Agreement, as well as any other provisions that by their nature should survive, shall survive any termination of this Agreement.

g) **Waiver.** A Party's failure or delay in exercising any right, power, or privilege under this Agreement, whether explicit or by lack of enforcement, shall not operate as a waiver, nor shall any single or partial exercise of any right, power, or privilege preclude any other or further exercise of such right, power, or privilege.

h) **Legal Requests.** Transferring Agency acknowledges and agrees that Recipient, or its contractors, may be required to share the Data to respond to a subpoena, court order, open records request or valid legal request (each a "Legal Request"). To the extent permitted by law, Recipient will refer the Legal Request to Transferring Agency of any disclosure of the Data so that Transferring Agency may seek a protective order at its own cost.

i) **CORA Disclosure**. To the extent not prohibited by federal law, this Agreement and the performance measures and standards required under §24-106-107, C.R.S., if any, are subject to public release through the Colorado Open Records Act.

a) **Governmental Immunity**. Liability for claims for injuries to persons or property arising from the negligence of the State, its departments, boards, commissions committees, bureaus, offices, employees and officials shall be controlled and limited by the provisions of the Colorado Governmental Immunity Act, §24-10-101, *et seq*., C.R.S.; the Federal Tort Claims Act, 28 U.S.C. Pt. VI, Ch. 171 and 28 U.S.C. 1346(b), and the State's risk management statutes, §§24-30-1501, *et seq*. C.R.S. No term or condition of this Agreement shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protections, or other provisions, contained in these statutes.

b) **Independent Contractor**. Recipient shall perform its duties hereunder as an independent contractor and not as an employee. Neither Recipient nor any agent or employee of Recipient shall be deemed to be an agent or employee of the State. Recipient shall not have authorization, express or implied, to bind the State to any agreement, liability or understanding, except as expressly set forth herein.

c) **Third-Party Beneficiaries**. None of the provisions of this Agreement shall be for the benefit of, or enforceable by, any third-party.

d) **Compliance with Law**. Recipient shall comply with all applicable federal and State laws, rules, and regulations in effect or hereafter established, including, without limitation, HIPAA.

e) **Choice of Law, Jurisdiction and Venue**. Colorado law, and rules and regulations issued pursuant thereto, shall be applied in the interpretation, execution, and enforcement of this Agreement. Any provision included or incorporated herein by reference that conflicts with said laws, rules, and regulations shall be null and void. All suits or actions related to this Agreement shall be filed and proceedings held in the State of Colorado and exclusive venue shall be in the City and County of Denver.

Appendix A

DATA TO BE SHARED

Data to be Shared

HCPF will deliver the following data ('SWSHE-eligible Coordinated Entry List') to Recipient (via an encrypted email) as an indication of Medicaid enrollees who HCPF deems eligible to participate in the Statewide Supportive Housing Expansion (SWSHE) Pilot Project.

1. Member First Name
2. Member Last Name
3. HMIS Unique Identifier

Recipient acknowledges and agrees that the Data is Protected Health Information that is protected pursuant to HIPAA and is subject to the additional terms in the Agreement that apply to Protected Health Information.