

## DELEGATION SERVICES ADDENDUM

This **Delegation Services Addendum (Addendum)** is made part of and incorporated into the **<Insert Type>** Participation Agreement entered into between **<Insert Name of the Humana or ChoiceCare entity>** (**Delegator**), and **<Insert Name>** (**Delegate**) which was effective **<Insert Effective date of Base Agreement>** (Agreement). This Addendum is intended to supplement the terms and conditions of the Agreement and to the extent that this Addendum conflicts with the terms and conditions of the Agreement, including any prior amendments, addenda, exhibits, or attachments, this Addendum controls the relationship between the parties.

The following Attachments are included with this Addendum and incorporated by reference herein:

**CONTRACTOR NOTE: Include only those Attachments that are appropriate for the Provider entity you are Delegating services to and delete the inapplicable Attachments – REMOVE THIS TEXT BEFORE SENDING TO DELEGATE.**

- A. Delegation of Credentialing Services Attachment
- B. Delegation of Utilization Review and Utilization Management Services Attachment
- C. Delegation of Complex Case Management
- D. Delegation of Disease Management
- E. Delegation of Claims Processing Attachment
- F. FDR Compliance Program Requirements Attachment (**required if being delegated for Medicare**)
- G. Process Integration Attachment (**required if being delegated for Claims**)
- H. IT Security Agreement Attachment (**required if being delegated for Claims and/or UM**)
- I. Business Associate Agreement Attachment (**required if Claims & UM are being delegated**)
- J. No Protected Health Information Certification Attachment (**required if being delegated only for Credentialing**)

### ARTICLE I DEFINITIONS

Any capitalized term in this Addendum or any of its Attachments not defined herein shall have the same meaning as set forth in the Agreement.

- 1.1 **Accreditation Organization** means any nationally recognized organization that accredits managed care organizations including without limitation to the National Committee of Quality Assurance (NCQA), the Utilization Review Accreditation Commission (URAC), and the Joint Commission (TJC) or other nationally recognized Accreditation Organization approved by Delegator.
- 1.2 **Subcontractor(s)** means any third party which has entered into an agreement with **Delegate** to perform part or all of **Delegate's** duties and/or obligations under this Addendum.

### ARTICLE II DELEGATE'S OBLIGATIONS

In order to fulfill the purposes and objective of this Addendum, the **Delegate** agrees:

- 2.1 To accept the obligation to perform all delegated functions and activities described in this Addendum and in each Attachment which are each incorporated by reference into the Agreement.
- 2.2 To comply with **Delegator's** policies, procedures, and program requirements, Member's Plan (coverage agreement), and all applicable state and federal laws, rules and regulations and instructions including but not limited to the CMS Standards and Accreditation Organization requirements pertaining to all functions and activities described in each Attachment.

- a. **Delegate** agrees to monitor all providers, employees and Subcontractors supporting any Medicare and/or Medicaid lines of business for debarments and exclusions from federal and state government programs. This must be conducted upon initial hire or contract and on a monthly basis thereafter. Accurate records of such monitoring activity must be maintained and retained for a period of a minimum of ten (10) years. Any provider, Subcontractor or employee found excluded from any Federal and state government program must be removed from providing direct or indirect services for Medicare/Medicaid or other state or federal governmental program Members immediately and shall be reported promptly to the **Delegator**.
  - b. **Delegate** further agrees to make available to **Delegator**, its designee or any state or federal governmental agency all documents, including but not limited to logs, files, committee meeting minutes and reports required within the timeframe determined by the auditor.
- 2.3 To furnish, at no expense to **Delegator**, any and all staffing and systems necessary to receive from and transmit to **Delegator**, or its designee, all required data, and will allow access to and provide to **Delegator**, or its designee, all data required by state and federal laws, rules and regulations, and **Delegator** or Accreditation Organization standards including without limitation any documentation, records, files or data necessary to perform the functions delegated under this Addendum.
- 2.4 That upon the termination of performance of delegated function under this Addendum, and/or the expiration, non-renewal or termination of the Addendum, regardless of the cause, any files, records and documentation or quality copies of such files and documentation pertaining to **Delegator's** Members or providers which are necessary for **Delegator** to resume responsibility for the delegated function will be made available to **Delegator** upon request.
- 2.5 To prepare and maintain all appropriate records which involve transactions relating to any services delegated hereunder in accordance with prudent and professional record-keeping procedures and as required by applicable federal, state, or local laws, rules, or regulations and **Delegator** or Accreditation Organization standards.
- 2.6 That, in the event that **Delegator** is financially penalized or incurs any administrative fine or penalty imposed by any state or federal agency or Accreditation Organization as a direct result of **Delegate's** or any of its employees or Subcontractor's failure to adhere to the applicable state or federal laws or regulations, or the standards and procedures described herein, **Delegator** will forward to **Delegate** documentation of such financial penalty and/or sanction, and **Delegate** shall reimburse **Delegator** the full amount of such financial penalty imposed, including without limitation any attorneys' fees incurred as a result of such action and penalty by a state or federal agency within thirty (30) calendar days of receipt of the documentation.
- 2.7 That notwithstanding anything to the contrary herein, this Addendum may not be construed to limit in any way the authority or responsibility of **Delegator** to comply with all state and federal laws, rules and regulations, and Accreditation Organization requirements to which **Delegator** is subject or be construed to limit in any way the authority of **Delegator's** Board of Directors to appoint, remove or change officers or employees of **Delegator**.
- 2.8 That all books, records, assets and liabilities of **Delegator** shall, at all times, remain the property of the **Delegator**.
- 2.9 To promptly notify **Delegator**, or its designee, in writing of any confirmed quality or risk issues of which **Delegate** may become aware of as it relates to the services delegated hereunder.
  - a. **Delegate** shall notify and provide documentation to **Delegator** within the next business day of any corrective action plan and/or sanctions, fines or other penalties imposed on or incurred by **Delegate**, or if applicable its Subcontractor, following any review by a regulatory agency or Accreditation Organization.

- b. **Delegate** agrees any material change in **Delegate's** performance of delegated functions shall be submitted to **Delegator** for review and approval by **Delegator** prior to the effective date of the proposed changes.
- 2.10 That **Delegator** may request a change or revision to the **Delegate's** programs and/or processes at any time as necessary to reflect changes in regulatory, **Delegator's** and/or Accreditation Organization requirements. Required changes or revisions will be provided to **Delegate** in writing, to be effective within ninety (90) calendar days, or such lesser period of time as may be required by applicable regulatory and/or Accreditation Organization requirements to which **Delegator** is subject. **Delegate** shall provide evidence of implementation to **Delegator** as directed.

### ARTICLE III ACCESS, AUDIT AND OVERSIGHT

**Delegate** agrees that state, federal and Accreditation Organization regulations or standards require **Delegator** to maintain oversight of the delegated functions furnished by **Delegate**. Such oversight shall, at a minimum, include:

- 3.1 **Delegator's** or its designee's right to conduct on-site visits at least annually, or more frequently if deemed necessary by **Delegator**, upon not less than ten (10) business days prior notice, or such shorter notice as may be imposed on **Delegator** by a state or federal regulatory agency or Accreditation Organization.
- 3.2 **Delegator**, **Delegator's** designee, federal, state, and local governmental authorities having jurisdiction, and/or Accreditation Organization to audit any and all documents and materials including, but not limited to, books, contracts, computer and other electronic systems, related to services rendered under this Addendum. **Delegate** shall also permit review of **Delegate's** policies and procedures, programs, annual plans, annual evaluation of previous year's programs, reports, and meeting minutes that have been approved by the **Delegate's** administrative/quality committee, and **Delegate's** performance/compliance under each Attachment.
- 3.3 Permission for **Delegator**, **Delegator's** designee, federal, state and local governmental authorities having jurisdiction, and/or Accreditation Organization's right to conduct a site visit and/or audit at any site at any time where **Delegate** performs delegated functions under the terms of this Addendum. Any such audit shall be permitted during the term of this Addendum and for a period of ten (10) years thereafter (or any greater period required by applicable law). This section shall survive the termination of this Addendum, regardless of the cause of termination;
- 3.4 Submission to **Delegator** of periodic reports. These reports shall be provided in accordance with the applicable delegated function attachment and at such other times as **Delegator** shall request or as **Delegator** shall deem necessary or appropriate to ensure that **Delegator** is fully apprised of **Delegate's** activities;
- 3.5 That **Delegate** agrees to retain all data, information, records, and documentation related to its performance of each delegated function under this Addendum for the longer of ten (10) years following the date of service or the period required by applicable state law.
- 3.6 **Delegate's** obligation to cooperate and comply with any Corrective Action Plan (CAP) established by **Delegator** in the event there is any breach of this Addendum or non-compliance with state or federal law, Accreditation Organization requirements or **Delegator's** policies and procedures. Corrective action may include, without limitation, intensifying the frequency and number of audits, the temporary loss of delegated rights under this Addendum or the termination of this Addendum.
- 3.7 **Delegate's** agreement that notwithstanding anything to the contrary herein, **Delegator**, in its sole discretion, or any state or federal regulatory authority, retains the right to approve, modify, suspend or revoke at any time all, or any portion, of functions and/or activities delegated hereunder.

- 3.8 **Delegate's** acknowledgement and agreement that **Delegator** reserves the right to perform assessments to review the effectiveness of **Delegate's** ability to perform the assigned delegated functions and compliance with established criteria. **Delegator** shall provide at least ten (10) business days prior written notice before conducting any onsite assessment.

#### **ARTICLE IV SUB-DELEGATION**

- 4.1 If **Delegate** sub-delegates any portion of the delegated functions to a Subcontractor, **Delegate** will require by contract that those functions shall be pre-approved by **Delegator** and be subject to the terms of this Addendum and will be provided in accordance with **Delegator's** policies, procedures and program requirements and all state and federal regulatory and/or Accreditation Organization requirements applicable to **Delegator**.
- 4.2 Such sub-delegation shall not relieve **Delegate** of its obligations under this Addendum. **Delegate** acknowledges and agrees that all of its obligations under this Addendum shall apply equally to any Subcontractor that provides any services under this Addendum, and **Delegate** represents and warrants that **Delegate** shall take all steps necessary to cause such Subcontractor to comply with the terms of this Addendum.
- 4.3 If **Delegate** sub-delegates any portion of the delegated functions, then **Delegate** will provide to **Delegator** documentation, and demonstrate a plan for adequate oversight of, Subcontractor prior to any sub-delegation and annually thereafter, or will provide to **Delegator**, in writing **Delegate's** request and acknowledgement that **Delegator** will perform oversight of all sub-delegated functions.
- 4.4 **Delegate** agrees to require by contract that Subcontractor acknowledge and agree that **Delegator** retains the right to perform evaluation and oversight of the Subcontractor, and will review or audit as required by law or if deemed necessary by **Delegator**.
- 4.5 The **Delegate** will provide **Delegator** with documentation of a written sub-delegation agreement and Business Associate Agreement that:
- a. Is mutually agreed upon;
  - b. Describes the responsibilities of the **Delegate** and Subcontractor;
  - c. Describes all sub-delegated activities;
  - d. Requires at least semi-annual reporting to the **Delegate**;
  - e. Describes the process by which the **Delegate** will regularly evaluate the Subcontractor's performance;
  - f. Describes the remedies, including revocation of the sub-delegation agreement, available to the **Delegate** if the Subcontractor does not fulfill its obligations.
- 4.6 If **Delegate** sub-delegates any portion of the delegated functions to a Subcontractor, then **Delegate** will require by contract that Subcontractor agrees to indemnify and hold **Delegator** and its affiliates and their respective agents, employees, and/or officers harmless from any and all claims, losses, liabilities, damages, injunctions, lawsuits, fines, penalties, demands and/or expenses of any kind or nature, including without limitation attorneys' fees, arising out of or in relation to Subcontractor's performance of the sub-delegated functions.
- 4.7 The **Delegate** agrees to monitor the Subcontractor for federal and state government programs exclusions on a monthly basis for Medicare/Medicaid providers and will maintain accurate records of such monitoring activity. Any provider, Subcontractor or employee found excluded from any Federal and/or state government program must be removed from providing direct or indirect services for Medicare/Medicaid or other governmental program Members immediately and shall be reported to the **Delegator**.

**ARTICLE V  
TERM AND TERMINATION**

- 5.1 This Addendum shall commence at 12:01 AM on the Effective Date specified below and shall continue in full force and effect for an initial term of twelve (12) months. This Addendum shall continue in full force and effect for additional twelve (12) month periods unless terminated in accordance with the terms outlined in the Agreement or this Addendum.
- 5.2 Notwithstanding anything to the contrary in this Addendum, the Attachments, or the Agreement, performance under this Addendum may be terminated without cause by either party upon written notice provided to the other party no less than ninety (90) calendar days prior written notice or by mutual agreement.
- 5.3 **Delegate** acknowledges that **Delegator** will provide ninety (90) days written notice of termination to the insurance commissioner if required by State law.
- 5.4 Notwithstanding anything else in this Addendum, the Attachments, or the Agreement any breach related to Delegate's accreditation, licensure, and/or quality assurance issues shall be considered non-curable. Furthermore, a determination by Delegator that Delegate's continued performance of the delegated functions and/or activities under this Addendum may adversely affect the health, safety or welfare of any Member or bring Delegator or its provider networks in to disrepute, shall be considered non-curable.
- 5.5 Notwithstanding any other provision in the Agreement, this Addendum or any Attachment, **Delegator** may terminate this Addendum, or any Attachment immediately and automatically without additional notice in the event **Delegator** determines that there has been any change or limitation that materially affects **Delegate's** ability to adequately deliver the services delegated hereunder, or for any of the reasons outlined in the Agreement.
- 5.6 This Addendum, including its Attachments and addenda hereto and the documents incorporated therein, constitutes the entire agreement between **Delegator** and **Delegate** with respect to the subject matter hereof, and it supersedes any and all prior or contemporaneous agreements, oral or written, regarding the subject matter hereof, between **Delegator** and **Delegate**.

The Effective Date of this Addendum is:           <Insert Date>          .

Each party to this Addendum represents that it has full power and authority to enter into this Addendum and the person signing this Addendum on behalf of either party represents that he/she has been duly authorized to enter into this Addendum.

**Delegate**

**Delegator**

By: \_\_\_\_\_  
Signature of Delegate

By: \_\_\_\_\_  
Signature of Delegator

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Printed Name

\_\_\_\_\_  
Title

\_\_\_\_\_  
Title

\_\_\_\_\_  
Date

\_\_\_\_\_  
Date

**DELEGATION OF CREDENTIALING SERVICES  
ATTACHMENT A**

**[PRACTITIONER ONLY TEMPLATE]**

This **Delegation of Credentialing Services Attachment** (“Credentialing Attachment”) is hereby made part of and incorporated into the Agreement and the Delegation Services Addendum, entered into by and between **<Insert Name of the Humana or ChoiceCare entity>** (**Delegator**), and **<Insert Name>** (**Delegate**). This Credentialing Attachment is intended to amend the terms and conditions of the Addendum and to the extent that this Credentialing Attachment conflicts with the terms and conditions of the Agreement or the Addendum, including any prior agreements, addenda, exhibits, or attachments, this Credentialing Attachment controls the relationship between the parties.

**ARTICLE I  
DELEGATE’S OBLIGATIONS**

**Delegate** agrees that it will:

- 1.1 Acknowledge and agree that **Delegate’s** credentialing policies and procedures, are subject to **Delegator’s** review and written approval prior to any delegation of credentialing functions.
- 1.2 Accept responsibility and the obligation for all delegated credentialing and recredentialing functions and activities in **TABLE 1**, which is included hereto and is incorporated by reference, as they relate to **Delegate’s** employed and / or contracted practitioners who are or will be rendering services to Members. All delegated credentialing and recredentialing functions and activities shall be carried out in accordance with the obligations in the Addendum and this Attachment.
- 1.3 Cooperate and comply with the standards and requirements provided by **Delegator**, which will be updated from time to time, including, but not limited to, the credentialing criteria and credentialing policies. **Delegate** further represents and acknowledges that Delegate's credentialing and recredentialing program, policies and processes must meet or exceed the standards and criteria requirements set forth by **Delegator**.
- 1.4 Maintain a credentialing committee, a credentialing and recredentialing program, and all related policies procedures and processes in compliance with state and federal law and Accreditation Organization requirements as they may be amended from time to time.
- 1.5 **Delegate** shall cooperate with **Delegator’s** efforts to implement quality improvement and other activities related to the credentialing and recredentialing program.
- 1.6 Acknowledge that **Delegator**, or its designee, retains the right to approve or deny new or renewing practitioner and to terminate or suspend individual practitioners from participation in any of **Delegator’s** networks. **Delegator** retains the ultimate responsibility for the credentialing and recredentialing of all providers in any of **Delegator’s** networks.
- 1.7 Acknowledge and agree that all practitioners must be fully credentialed/recruentialed by the **Delegate** prior to rendering any services to Members.
- 1.8 Obtain, evaluate, verify and provide to **Delegator** or its designee, upon request, any and all information necessary and appropriate for the credentialing of applicants and recredentialing of Participating Providers. All verifications shall be thoroughly documented according to state and federal law and Accreditation Organization requirements.
- 1.9 Provide a complete report of all Participating Providers credentialed and/or recruentialed by **Delegate** on a semi-annual basis to **Delegator**. All reports are to be sent via secured email to your assigned delegation compliance consultant. **Delegate** shall include the elements indicated below in all credentialing reports:

- |  |
|--|
| <p><b>Practitioner Reports:</b></p> <ul style="list-style-type: none"><li>• Practitioner</li><li>• Degree</li><li>• Practicing Specialty</li><li>• NPI Number</li><li>• Initial Credentialing Date</li><li>• Last Recredentialing Date</li><li>• Specialist/Hospitalist Indicator</li><li>• State of Practice</li><li>• Active Hospital Privileges (if applicable)</li></ul> |
|--|

- 1.10 In addition, **Delegate** shall submit reports containing all credentialing approvals and denials to **Delegator's** appropriate network operations department within thirty (30) calendar days of the credentialing decision date.
- 1.11 Acknowledge that **Delegator** retains all other credentialing functions not specified as the **Delegate's** responsibility in this Attachment.

**ARTICLE II  
ACCESS, AUDIT AND OVERSIGHT**

**Delegate** agrees that it shall:

- 2.1 At least annually, or more frequently if deemed necessary by **Delegator**, and then upon not less than ten (10) business days prior notice, or such shorter notice as may be imposed on **Delegator** by a federal or state regulatory agency or Accreditation Organization, allow **Delegator**, its designee, and any state or federal entity or Accreditation Organization to access all credentialing/recredentialing documentation, processes, policies, systems, and credentialing/ recredentialing files in order to permit **Delegator**, or its designee, to perform an audit review of the **Delegate's** credentialing and recredentialing performance / compliance under this Credentialing Attachment. This includes, but is not limited to, a review of any credentialing and/or recredentialing files, credentialing and recredentialing policies and procedures, and committee meeting minutes that have been approved by the **Delegate's** credentialing committee. **Delegator** will provide at least a ten (10) business days notification on annual audits. The notification for state or federal entity or Accreditation Organization audits will depend on the timeframe imposed on **Delegator**, by state or federal entity or Accreditation Organization. This provision will survive the termination of this Credentialing Attachment for a period of one full credentialing or recredentialing cycle. In-person or telephonic/virtual meetings with participation of both **Delegator** and the **Delegate** will be held to discuss results of audits or reports on an as needed basis.
- 2.2 Agree that all elements of credentialing and/or recredentialing activities and all functions delegated hereunder require a minimum of ninety-five percent (95%) compliance. Failure to meet compliance requirements described above will result minimally in a Corrective Action Plan ("**CAP**"), and may result in revocation of some or all of the delegated activities.
- a. A CAP issued by **Delegator** will include the issues identified, actions which are required to be taken, submission due dates and methods of re-evaluation, and may also include without limitation, intensifying the frequency and number of on-site audits, the temporary loss of some or all delegated rights under this Credentialing Attachment, or the termination of the Addendum.
  - b. **Delegate** will have fourteen (14) calendar days to provide a written response describing how they will meet the requirements found to be noncompliant including prospective date of compliance.
  - c. If **Delegator** receives information through its monitoring plan and/or audit processes, or otherwise, that **Delegate** or its Subcontractors are not operating in accordance with the terms of this

Credentialing Attachment, **Delegator** may issue a CAP to **Delegate**, or may revoke delegated credentialing activities.

- d. Failure of the **Delegate** to comply with the terms of a CAP in the required timeframes may result in revocation of any one or all delegated activities, and/or termination of this Credentialing Attachment.

### **ARTICLE III TERMINATION**

- 3.1 Notwithstanding anything to the contrary in this Credentialing Attachment, the Delegation Services Addendum, or the Agreement, performance under this Attachment may be terminated without cause by either party upon written notice provided to the other party no less than ninety (90) calendar days preceding the termination date or by mutual agreement.
- 3.2 Notwithstanding anything else in this Credentialing Attachment, any breach related to accreditation and/or licensure, quality assurance issues or alleged breach regarding termination by **Delegator** in the event **Delegator** determines that **Delegate's** continued performance of the delegated functions and/or activities under this Credentialing Attachment may affect adversely the health, safety or welfare of any Member or bring **Delegator** or its provider networks in to disrepute, shall be considered non-curable.
- 3.3 Upon termination of the Delegation Services Addendum or this Credentialing Attachment, **Delegate** will provide **Delegator** with a list of all credentialed or recredentialed Participating Providers, the date when each Participating Provider was last credentialed or recredentialed, a summary of all credentials that were verified, and an attestation stating that each Participating Provider met all required **Delegator** credentialing/reccredentialing criteria as of the last date each Participating Provider was credentialed or recredentialed.

The Effective Date of this Attachments is:           <Insert Date>          .

**TABLE 1**  
**Credentialing & Recredentialing Requirements**

| Practitioner Credentialing  | Responsibility of Delegate | Responsibility of Delegator |
|---|----------------------------|-----------------------------|
| a. Verification of current, valid state license(s)  | X                          |                             |
| b. Verification of current, valid DEA or CDS certificate(s)   | X                          |                             |
| c. Verification of education and training at initial credentialing, if not board certified  | X                          |                             |
| d. Verification of board certification, if applicable   | X                          |                             |
| e. Collection of five (5) year work history at initial credentialing  | X                          |                             |
| f. Verification of National Practitioner Data Bank (NPDB)*  | X                          |                             |
| g. Verification of professional liability claims history  | X                          |                             |
| h. Verification of state license sanctions or restrictions  | X                          |                             |
| i. Verification of Medicare and Medicaid sanctions <ul style="list-style-type: none"> <li>• DHHS OIG List of Excluded Individuals and Entities (LEIE), or</li> <li>• NPDB query</li> </ul>  | X                          |                             |
| j. Verification of Medicare Opt-Out*  | X                          |                             |
| k. Verification of Clinical Privileges*   | X                          |                             |
| l. Collection of current malpractice insurance coverage   | X                          |                             |
| m. Verification of Medicare and Medicaid Eligibility* <ul style="list-style-type: none"> <li>• GSA Excluded Parties Lists System (EPLS)/SAM, and</li> <li>• Any applicable state eligibility or exclusion list</li> </ul>   | X                          |                             |
| n. Collection of applications, reapplications and signed attestation that addresses: <ul style="list-style-type: none"> <li>• Inability to perform the essential functions of the position,</li> <li>• Lack of present illegal drug use,</li> <li>• History of loss of license and felony conviction,</li> <li>• History of loss or limitation of privileges or disciplinary activity,</li> <li>• Signed and dated attestation to the correctness and completeness,</li> <li>• Signed and dated consent form, and</li> <li>• State Mandated application, if applicable</li> </ul> | X                          |                             |
| o. Performance monitoring at recredentialing:* <ul style="list-style-type: none"> <li>• Information from quality improvement activities, and</li> <li>• Member complaints</li> </ul>  | X                          |                             |
| p. Credentials Committee review/decision  | X                          |                             |
| q. Practitioner appeals process   | X                          |                             |
| r. Conduct site visits that are required by law to be completed as part of the initial or recredentialing file, if required by your state   | X                          |                             |
| s. Collect and evaluate ongoing monitoring of sanctions and complaints <ul style="list-style-type: none"> <li>• Complaints,</li> <li>• Medicare/Medicaid sanctions,</li> <li>• State license sanctions,</li> <li>• Medicare Opt-Out*, and</li> <li>• Medicare and Medicaid Eligibility*</li> </ul>  |                            | X                           |
| t. Conduct oversight audits   |                            | X                           |

Attachment I.C.1-5 Delegation Services Addendum Delegation

|   |  |   |
|---|--|---|
| u. Retain the right to approve, deny, terminate or suspend new or renewing practitioners and organizational providers from participation in any of Delegator's networks |  | X |
| v. Collects semi-annual reports   |  | X |

\*Medicare and/or Medicaid Only

**DELEGATION OF CREDENTIALING SERVICES  
ATTACHMENT A**

**[ORGANIZATIONAL ONLY TEMPLATE]**

This **Delegation of Credentialing Services Attachment** (“Credentialing Attachment”) is hereby made part of and incorporated into the Agreement and the Delegation Services Addendum, entered into by and between **<Insert Name of the Humana or ChoiceCare entity>** (**Delegator**), and **<Insert Name>** (**Delegate**). This Credentialing Attachment is intended to amend the terms and conditions of the Addendum and to the extent that this Credentialing Attachment conflicts with the terms and conditions of the Agreement or the Addendum, including any prior agreements, addenda, exhibits, or attachments, this Credentialing Attachment controls the relationship between the parties.

**ARTICLE I  
DELEGATE’S OBLIGATIONS**

**Delegate** agrees that it shall:

- 1.1 Acknowledge and agree that **Delegate’s** policies and procedures are subject to **Delegator’s** review and written approval prior to any delegation of credentialing functions.
- 1.2 Accept responsibility and the obligation for all delegated credentialing and recredentialing functions and activities in **TABLE 1**, which is included hereto and is incorporated by reference herein as it relates to **Delegate’s** organizational providers who are or will be rendering services to Members. All delegated credentialing and recredentialing functions and activities shall be carried out in accordance with the obligations in the Addendum and this Credentialing Attachment.
- 1.3 Agree to cooperate and comply with the standards and requirements provided by **Delegator**, which will be updated from time to time, including without limitation, the credentialing criteria and credentialing policies. **Delegate** further represents and acknowledges that Delegate's credentialing and recredentialing program, policies and processes must meet or exceed the standards and criteria requirements set forth by **Delegator**.
- 1.4 Maintain a credentialing committee, a credentialing and recredentialing program, and all related policies procedures and processes in compliance with state and federal law and Accreditation Organization requirements as they may be amended from time to time.
- 1.5 **Delegate** shall cooperate with **Delegator’s** efforts to implement quality improvement and other activities related to the credentialing and recredentialing program.
- 1.6 Acknowledge that **Delegator**, or its designee, retains the right to approve or deny new or renewing organizational providers and sites and to terminate or suspend organizational providers and sites from participation in any of **Delegator’s** networks. **Delegator** retains the ultimate responsibility for the credentialing and recredentialing of all providers in any of **Delegator’s** networks.
- 1.7 Acknowledge and agree that all organizational providers must be fully credentialed / recredentialed by the **Delegate** prior to rendering any services to Members.
- 1.8 Obtain, evaluate, verify and provide to **Delegator** or its designee, upon request, any and all information necessary and appropriate for the credentialing of applicants and recredentialing of participating organizational providers. All verifications shall be thoroughly documented according to state and federal law and Accreditation Organization requirements.
- 1.9 Provide a complete report of all participating organizational providers credentialed and/or recredentialed by **Delegate** on a semi-annual basis to **Delegator**. All reports are to be sent via secured email to your assigned delegation compliance consultant. **Delegate** shall include the elements indicated below in all credentialing reports:

**Organizational Provider Reports:**

- Organizational Provider Name
- Organizational Provider Type
- NPI Number
- Initial Credentialing Date
- Last Recredentialing Date
- State of Organizational Provider Location

- 1.10 In addition, **Delegate** shall submit reports containing all credentialing approvals and denials to **Delegator's** appropriate network operations department within thirty (30) calendar days of the credentialing decision date.
- 1.11 Acknowledge that **Delegator** retains all other credentialing functions not specified as the **Delegate's** responsibility in this Credentialing Attachment.

## ARTICLE II ACCESS, AUDIT AND OVERSIGHT

**Delegate** agrees that it shall:

- 2.1 At least annually, or more frequently if deemed necessary by **Delegator**, and then upon not less than ten (10) business days prior notice, or such shorter notice as may be imposed on **Delegator** by a federal or state regulatory agency or Accreditation Organization, allow **Delegator**, its designee, and any state or federal entity or Accreditation Organization to access all credentialing/recredentialing documentation, processes, policies, systems, and credentialing/recredentialing files in order to perform an audit review of the **Delegate's** credentialing and recredentialing performance/compliance under this Credentialing Attachment. This includes, but is not limited to, a review of any credentialing and/or recredentialing files, credentialing and recredentialing policies and procedures, and committee meeting minutes that have been approved by the **Delegate's** credentialing committee. **Delegator** will provide at least a ten (10) business days notification on annual audits. The notification for state or federal entity or Accreditation Organization audits will depend on the timeframe imposed on **Delegator** by state or federal entity or Accreditation Organization. This provision will survive the termination of this Credentialing Attachment for a period of one full credentialing or recredentialing cycle. In-person or telephonic / virtual meetings with participation of both **Delegator** and the **Delegate** will be held to discuss results of audits or reports on an as needed basis.
- 2.2 Agree that all elements of credentialing and/or recredentialing activities and all functions delegated hereunder require a minimum of ninety-five percent (95%) compliance. Failure to meet compliance requirements described above will result minimally in a Corrective Action Plan ("**CAP**"), and may result in revocation of some or all of the delegated activities.
- a. A CAP issued by **Delegator** will include the issues identified, actions which are required to be taken, submission due dates and methods of re-evaluation, and may also include without limitation, intensifying the frequency and number of on-site audits, the temporary loss of some or all delegated rights under this Credentialing Attachment, or the termination of the Addendum.
  - b. **Delegate** will have fourteen (14) calendar days to provide a written response describing how they will meet the requirements found to be noncompliant including prospective date of compliance.

- c. If **Delegator** receives information through its monitoring plan and/or audit processes, or otherwise, that **Delegate** or its Subcontractors are not operating in accordance with the terms of this Credentialing Attachment, **Delegator** may issue a CAP to **Delegate**, or may revoke delegated credentialing activities.
- d. Failure of the **Delegate** to comply with the terms of a CAP in the required timeframes may result in revocation of any one or all delegated activities, and/or termination of this Credentialing Attachment.

**ARTICLE III  
TERMINATION**

- 3.1 Credentialing Attachment may be terminated without \_\_\_\_\_ cause by either party upon written notice provided to the other party no less than ninety (90) calendar days preceding the termination date or by mutual agreement.
- 3.2 Notwithstanding anything else in this Credentialing Attachment, any breach related to accreditation and/or licensure, quality assurance issues or alleged breach regarding termination by **Delegator** in the event **Delegator** determines that **Delegate**'s continued performance of the delegated functions and/or activities under this Credentialing Attachment may affect adversely the health, safety or welfare of any Member or bring **Delegator** or its provider networks in to disrepute, shall be considered non-curable.
- 3.3 Upon termination of the Delegation Services Addendum or this Credentialing Attachment, **Delegate** will \_\_\_\_\_ provide **Delegator** with a list of all credentialed or recredentialed Participating Providers , the date when each participating organizational provider was last credentialed or recredentialed, a summary of all credentials that were verified, and an attestation stating that each participating organizational provider met all required **Delegator** credentialing/reccredentialing criteria as of the last date each participating organizational provider was credentialed or recredentialed .

The **Effective Date** of this Credentialing Attachment is:                     <Insert Date>                    .

**TABLE 1**  
**Organizational Provider Requirements**

| Organizational Provider Credentialing   | Responsibility of Delegate | Responsibility of Delegator |
|---|----------------------------|-----------------------------|
| • Copy of current state license   | X                          |                             |
| • Copy of current accreditation certificate (if applicable)   | X                          |                             |
| • Copy of current Medicare/Medicaid certificate (if applicable)   | X                          |                             |
| • Medicare sanctions query  | X                          |                             |
| • Accreditation, Medicare certification or site visit   | X                          |                             |
| • Conduct oversight audits  |                            | X                           |
| • Retain the right to approve, deny, terminate or suspend new or renewing practitioners and organizational providers from participation in any of Delegator's networks. |                            | X                           |
| • Collects semi-annual reports  |                            | X                           |

## DELEGATION OF CREDENTIALING SERVICES ATTACHMENT A

### [PRACTITIONER AND ORGANIZATION TEMPLATE]

This **Delegation of Credentialing Services Attachment** (“Credentialing Attachment”) is hereby made part of and incorporated into the Agreement and the Delegation Services Addendum, entered into by and between **<Insert Name of the Humana or ChoiceCare entity> (Delegator)**, and **<Insert Name> (Delegate)**. This Credentialing Attachment is intended to amend the terms and conditions of the Addendum and to the extent that this Credentialing Attachment conflicts with the terms and conditions of the Agreement or the Addendum, including any prior agreements, addenda, exhibits, or attachments, this Credentialing Attachment controls the relationship between the parties.

### ARTICLE I DELEGATE’S OBLIGATIONS

**Delegate** agrees that it shall:

- 1.1 Acknowledge and agree that **Delegate’s** policies and procedures are subject to **Delegator’s** review and written approval prior to any delegation of credentialing functions.
- 1.2 Accept responsibility and the obligation for all delegated credentialing and recredentialing functions and activities. Delegated credentialing and recredentialing functions and activities in **TABLE 1 and TABLE 2**, which are included hereto and are incorporated by reference herein as they relate to **Delegate’s** employed and/or contracted practitioners and organizational providers who are or will be rendering services to Members. All delegated credentialing and recredentialing functions and activities shall be carried out in accordance with the obligations in the Addendum and this Credentialing Attachment.
- 1.3 Agree to cooperate and comply with the standards and requirements provided by **Delegator**, which will be updated from time to time, including, but not limited to, the credentialing criteria and credentialing policies. **Delegate** further represents and acknowledges that Delegate’s credentialing and recredentialing program, policies and processes must meet or exceed the standards and criteria requirements set forth by **Delegator**.
- 1.4 Maintain a credentialing committee, a credentialing and recredentialing program, and all related policies procedures and processes in compliance with state and federal law and Accreditation Organization requirements as they may be amended from time to time.
- 1.5 **Delegate** shall cooperate with **Delegator’s** efforts to implement quality improvement and other activities related to the credentialing and recredentialing program.
- 1.6 Acknowledge that **Delegator retains** the right to approve or deny new or renewing practitioners and organizational providers and sites and to terminate or suspend individual practitioners and organizational providers and sites from participation in any of **Delegator’s** networks. **Delegator** retains the ultimate responsibility for the credentialing and recredentialing of all providers in any of **Delegator’s** networks.
- 1.7 Acknowledge and agree that all practitioners and organizational providers must be fully credentialed/recruentialed by the **Delegate** prior to rendering any services to Members.
- 1.8 Obtain, evaluate, verify and provide to **Delegator** or its designee, upon request, any and all information necessary and appropriate for the credentialing of applicants and recredentialing of Participating Providers. All verifications shall be thoroughly documented according to state and federal law and Accreditation Organizational requirements.
- 1.9 Provide a complete report of all Participating Providers credentialed and/or recruentialed by **Delegate** on a semi-annual basis to **Delegator**. All reports are to be sent via secured email to your assigned delegation compliance consultant. **Delegate** shall include the elements indicated below in all credentialing reports:

|  |   |
|--|---|
| <p><b>Practitioner Reports:</b></p> <ul style="list-style-type: none"> <li>• Practitioner</li> <li>• Degree</li> <li>• Practicing Specialty</li> <li>• NPI Number</li> <li>• Initial Credentialing Date</li> <li>• Last Recredentialing Date</li> <li>• Specialist/Hospitalist Indicator</li> <li>• State of Practice</li> <li>• Active Hospital Privileges (if applicable)</li> </ul> | <p><b>Organizational Provider Reports:</b></p> <ul style="list-style-type: none"> <li>• Organizational Provider Name</li> <li>• Organizational Provider Type</li> <li>• NPI Number</li> <li>• Initial Credentialing Date</li> <li>• Last Recredentialing Date</li> <li>• State of Organizational Provider Location</li> </ul> |
|--|---|

- 1.10 In addition, **Delegate** shall submit reports containing all credentialing approvals and denials to **Delegator's** appropriate network operations department within thirty (30) calendar days of the credentialing decision date.
- 1.11 Acknowledge that **Delegator** retains all other credentialing functions not specified as the **Delegate's** responsibility in this Credentialing Attachment.

**ARTICLE II  
ACCESS, AUDIT AND OVERSIGHT**

**Delegate** agrees that it shall:

- 2.1 At least annually, or more frequently if deemed necessary by **Delegator**, and then upon not less than ten (10) business days prior notice, or such shorter notice as may be imposed on **Delegator** by a federal or state regulatory agency or Accreditation Organization, allow **Delegator**, its designee, and any state or federal entity or Accreditation Organization to access all credentialing/recredentialing documentation, processes, policies, systems, and credentialing/recredentialing files in order to perform an audit review of the **Delegate's** credentialing and recredentialing performance/compliance under this Credentialing Attachment. This includes, but is not limited to, a review of any credentialing and/or recredentialing files, credentialing and recredentialing policies and procedures, and committee meeting minutes that have been approved by the **Delegate's** credentialing committee. **Delegator** will provide at least a ten (10) business days notification on annual audits. The notification for state or federal entity or Accreditation Organization audits will depend on the timeframe imposed on **Delegator** by state or federal entity or Accreditation Organization. This provision will survive the termination of this Credentialing Attachment for a period of one full credentialing or recredentialing cycle. In-person or telephonic/virtual meetings with participation of both **Delegator** and the **Delegate** will be held to discuss results of audits or reports on an as needed basis.
- 2.2 Agree that all elements of credentialing and/or recredentialing activities and all functions delegated hereunder require a minimum of ninety-five percent (95%) compliance. Failure to meet compliance requirements described above will result minimally in a Corrective Action Plan ("**CAP**"), and may result in revocation of some or all of the delegated activities.
  - a. A CAP issued by **Delegator** will include the issues identified, actions which are required to be taken, submission due dates and methods of re-evaluation, and may also include without limitation, intensifying the frequency and number of on-site audits, the temporary loss of some or all delegated rights under this Credentialing Attachment, or the termination of the Addendum.
  - b. **Delegate** will have fourteen (14) calendar days to provide a written response describing how they will meet the requirements found to be noncompliant including prospective date of compliance.
  - c. If **Delegator** receives information through its monitoring plan and/or audit processes, or otherwise, that **Delegate** or its Subcontractors are not operating in accordance with the terms

of this Credentialing Attachment, **Delegator** may issue a CAP to **Delegate**, or may revoke delegated credentialing activities.

- d. Failure of the **Delegate** to comply with the terms of a CAP in the required timeframes may result in revocation of any one or all delegated activities, and/or termination of this Credentialing Attachment.

**ARTICLE III  
TERMINATION**

- 3.1 Credentialing Attachment may be terminated without \_\_\_\_\_ cause by either party upon written notice provided to the other party no less than ninety (90) calendar days preceding the termination date or by mutual agreement.
- 3.2 Notwithstanding anything else in this Credentialing Attachment, any breach related to accreditation and/or licensure, quality assurance issues or alleged breach regarding termination by **Delegator** in the event **Delegator** determines that **Delegate**'s continued performance of the delegated functions and/or activities under this Credentialing Attachment may affect adversely the health, safety or welfare of any Member or bring **Delegator** or its provider networks in to disrepute, shall be considered non-curable.
- 3.3 Upon termination of the Delegation Services Addendum or this Credentialing Attachment, **Delegate** will \_\_\_\_\_ provide **Delegator** with a list of all credentialed or recredentialed Participating Providers , the date when each Participating Provider was last credentialed or recredentialed, a summary of all credentials that were verified, and an attestation stating that each Participating Provider met all \_\_\_\_\_ required **Delegator** credentialing/reccredentialing criteria as of the last date each Participating Provider was credentialed or recredentialed .

The **Effective Date** of this Credentialing Attachment is:           <Insert Date>          .

**TABLE 1**  
**Credentialing & Recredentialing Requirements**

| Practitioner Credentialing  | Responsibility of Delegate | Responsibility of Delegator |
|---|----------------------------|-----------------------------|
| a. Verification of current, valid state license(s)  | X                          |                             |
| b. Verification of current, valid DEA or CDS certificate(s)   | X                          |                             |
| c. Verification of education and training at initial credentialing, if not board certified  | X                          |                             |
| d. Verification of board certification, if applicable   | X                          |                             |
| e. Collection of five (5) year work history at initial credentialing  | X                          |                             |
| f. Verification of National Practitioner Data Bank (NPDB)*  | X                          |                             |
| g. Verification of professional liability claims history  | X                          |                             |
| h. Verification of state license sanctions or restrictions  | X                          |                             |
| i. Verification of Medicare and Medicaid sanctions <ul style="list-style-type: none"> <li>• DHHS OIG List of Excluded Individuals and Entities (LEIE), or</li> <li>• NPDB query</li> </ul>  | X                          |                             |
| j. Verification of Medicare Opt-Out*  | X                          |                             |
| k. Verification of Clinical Privileges*   | X                          |                             |
| l. Collection of current malpractice insurance coverage   | X                          |                             |
| m. Verification of Medicare and Medicaid Eligibility* <ul style="list-style-type: none"> <li>• GSA Excluded Parties Lists System (EPLS)/SAM, and</li> <li>• Any applicable state eligibility or exclusion list</li> </ul>   | X                          |                             |
| n. Collection of applications, reapplications and signed attestation that addresses: <ul style="list-style-type: none"> <li>• Inability to perform the essential functions of the position,</li> <li>• Lack of present illegal drug use,</li> <li>• History of loss of license and felony conviction,</li> <li>• History of loss or limitation of privileges or disciplinary activity,</li> <li>• Signed and dated attestation to the correctness and completeness,</li> <li>• Signed and dated consent form, and</li> <li>• State Mandated application, if applicable</li> </ul> | X                          |                             |
| o. Performance monitoring at recredentialing:* <ul style="list-style-type: none"> <li>• Information from quality improvement activities, and</li> <li>• Member complaints (PCPs)</li> </ul>   | X                          |                             |
| p. Credentials Committee review/decision  | X                          |                             |
| q. Practitioner appeals process   | X                          |                             |
| r. Conduct site visits that are required by law to be completed as part of the initial or recredentialing file.   | X                          |                             |
| s. Collect and evaluate ongoing monitoring of sanctions and complaints <ul style="list-style-type: none"> <li>• Complaints,</li> <li>• Medicare/Medicaid sanctions,</li> <li>• State license sanctions,</li> <li>• Medicare Opt-Out*, and</li> <li>• Medicare and Medicaid Eligibility*</li> </ul>  |                            | X                           |
| t. Conduct oversight audits   |                            | X                           |

|   |  |   |
|---|--|---|
| u. Retain the right to approve, deny, terminate or suspend new or renewing practitioners and organizational providers from participation in any of Delegator’s networks |  | X |
| v. Collects semi-annual reports   |  | X |

\*Medicare and/or Medicaid Only

**TABLE 2**  
**Organizational Provider Requirements**

| <b>Organizational Provider Credentialing</b>  | <b>Responsibility of Delegate</b> | <b>Responsibility of Delegator</b> |
|---|-----------------------------------|------------------------------------|
| • Copy of current state license   | X                                 |                                    |
| • Copy of current accreditation certificate (if applicable)   | X                                 |                                    |
| • Copy of current Medicare/Medicaid certificate (if applicable)   | X                                 |                                    |
| • Medicare sanctions query  | X                                 |                                    |
| • Accreditation, Medicare certification or site visit   | X                                 |                                    |
| • Conduct oversight audits  |                                   | X                                  |
| • Retain the right to approve, deny, terminate or suspend new or renewing practitioners and organizational providers from participation in any of Delegator’s networks. |                                   | X                                  |
| • Collects semi-annual reports  |                                   | X                                  |

**DELEGATION OF UTILIZATION REVIEW  
AND UTILIZATION MANAGEMENT SERVICES for MEDICAL and/or BEHAVIORAL HEALTH  
SERVICES (BHS) (Remove BHS language if the delegate is not handling BH and remove  
instructions)  
ATTACHMENT**

This **Delegation of Utilization Review and Utilization Management Services Attachment** (“UM Attachment”) is hereby made part of and incorporated into the Agreement and the Delegation Services Addendum, entered into between **<Insert Name of the Delegator Humana entity> (Delegator)**, and **<Insert Name> (Delegate)** effective **< Date>**. This UM Attachment is intended to amend the terms and conditions of the Addendum and to the extent that this UM Attachment conflicts with the terms and conditions of the Agreement or the Addendum, including any prior agreements, addenda, exhibits, or attachments, this UM Attachment controls the relationship between the parties.

**ARTICLE I  
DELEGATE’S OBLIGATIONS**

**Delegate** agrees that it shall:

- 1.1 Acknowledge and agree that **Delegate’s** policies and procedures are subject to **Delegator’s** review and written approval prior to any delegation of utilization review and utilization management (collectively UR/UM) functions. .
- 1.2 Accept the responsibility and the obligation for performing all UR/UM delegated functions and activities specified in the **TABLE 1** and **Table 2**, which are attached hereto and incorporated by reference herein, as they relate to services rendered to Members assigned to physicians, employees, Subcontractors and independent contractors.
- 1.3 Ensure **Delegate’s** policies and procedures include provisions detailing **Delegate’s** oversight of all employed and contracted persons or entities that provide any functions or services delegated hereunder. **Delegate** shall ensure that all licensed Health Care Professionals shall provide Members all available health care services within the normal scope of and in accordance with their licenses and certifications under applicable state law.
- 1.4 **Delegate** shall utilize predetermined and nationally recognized criteria for clinical authorizations and / or referrals of Member services. A licensed registered nurse (RN) shall review authorizations and / or referrals that require clinical analysis and/or judgment and document such in the Member’s file.
- 1.5 Comply with **Delegator’s** policies, procedures, and program requirements and all applicable state and federal laws, rules and regulations and Accreditation Organization requirements pertaining to UR/UM and the delivery of medical and related health care services.
- 1.6 Demonstrate **Delegate’s** UR/UM program plan, previous plan evaluation, and subsequent revisions have been approved by **Delegate’s** internal quality/utilization review/management committees.
- 1.7 Maintain an internal quality, UR/UM management committee (UR/UM Committee) and UR/UM program, and will demonstrate that **Delegate’s** UR/UM program plan, previous plan evaluation, and subsequent revisions have been approved by **Delegate’s** UR/UM Committee.
- 1.8 Have and maintain policies and procedures and demonstrate oversight capability of all organizational providers, including, but not limited to, skilled nursing homes, hospitals, and ambulatory care centers not directly contracted with **Delegator** in accordance with **Delegator’s** policies and procedures (Provider Manual), Accreditation Organization standards, applicable laws, rules, and regulatory requirements.

- 1.9 Not provide incentives to deny, limit, or discontinue Medically Necessary services. Nothing contained in this UM Attachment or the Agreement is intended by **Delegator** to be a financial incentive or payment, which directly or indirectly acts as an inducement for the **Delegate** to limit Medically Necessary services.
- 1.10 Provide notification to **Delegator** of the termination of any **Delegate** Participating Provider.
- 1.11 Where a license, registration or certification is required by applicable law, rule or regulation or Accreditation Organizational requirement, provide **Delegator** a copy of **Delegate's** or its Subcontractor's utilization review license, registration and/or certification and its license/registration/certification number(s) prior to execution of this UM Attachment and upon renewal thereafter.
- 1.12 Use **Delegator** prepared Member letter templates for all delegated lines of business as indicated.
- 1.13 Retain all Member-related information and records created for a period of not less than ten (10) years.
- 1.14 Acknowledge that **Delegator** retains all other UM/UR functions not specified as the **Delegate's** responsibility in this UM Attachment .
- 1.15 The **Delegate** will manage Special Needs Plan Members, who are part of the **Delegate's** assigned membership from a UM/UR perspective. The **Delegate** must work with and coordinate care as directed by Humana at Home associates or other entity designated by **Delegator**.

## ARTICLE II ACCESS, AUDIT, AND OVERSIGHT

**Delegate** agrees that it shall:

- 2.1 At least annually, or more frequently if deemed necessary by **Delegator**, and then upon not less than ten (10) business days prior notice, or such shorter notice as may be imposed on **Delegator** by a federal or state regulatory agency or Accreditation Organization, allow **Delegator**, its designee, and any state or federal entity or Accreditation Organization to access all UR /UM documentation, processes, policies, systems, and files in order to perform an audit review of the **Delegate's** policies and procedures, program plan, UR/UM Committee meeting minutes that have been approved by the **Delegate's** UR/UM Committee, and **Delegate's** performance/compliance under this UM Attachment. In-person or telephonic/virtual meetings with participation of both **Delegator** and the **Delegate** will be held to discuss results of audits or reports on an as needed basis.
- 2.2 Submit to **Delegator**, with respect to delegated functions, all required reports and analyses including but not limited to the contents in **TABLE 3** which is attached hereto and incorporated herein by reference, along with identified problems, corrective actions initiated, and outcomes.
  - a. All reports and subsections of reports must be specific to line of business and all reporting formats must be pre-approved by **Delegator**.
  - b. **Delegate** agrees to provide any and all reports requested by **Delegator** within the timeframes identified by **Delegator** to ensure **Delegator** meets all new and revised **Delegator**, CMS, Federal, State and Accreditation Organization reporting requirements.
- 2.3 Make available to **Delegator** or their designee upon request, monthly service denial logs that will contain the information as indicated in **TABLE 4** as well as an analysis and summary of compliance to timeliness standards for requests and notification of denials.
- 2.4 Maintain a denial of service file for all types of delegated services including pre-service, concurrent, urgent/expedited and retrospective denials. The denial of service file must contain, at a minimum, the information found in **TABLE 5**.

- 2.5 Authorization files (expedited/urgent/standard/non-urgent) should include copies of the information found in TABLE 5.
- 2.6 Should the Delegate be placed on a corrective action plan(CAP), the Delegate will have up to fourteen (14) calendar days to provide a written response describing how they will meet the requirements found to be noncompliant including prospective date of compliance.
- 2.7 Delegate will be subject to a capitation payment penalty as indicated in the Table immediately below for any outstanding issues noted on a CAP.

| <b>Outstanding Corrective Action Plan</b> | <b>0 to 3 months</b> | <b>4-6 months</b>                      | <b>7-9 months</b>                      | <b>10-12 months or greater</b>         |
|---|----------------------|--|--|--|
| <b>Payment Penalty</b>                    | <b>0%</b>            | <b>1% per month until CAP resolved</b> | <b>2% per month until CAP resolved</b> | <b>3% per month until CAP resolved</b> |

**ARTICLE III  
MEMBER APPEALS AND GRIEVANCES/COMPLAINTS**

- 3.1 **Delegator’s** Member expedited and standard complaints/appeals/grievances are not delegated. **Delegator** maintains all Member rights and responsibility functions. **Delegator** will handle all Member appeals/ grievances/complaints for denied services including expedited and standard complaints/appeals/grievances made by a physician/practitioner on behalf of the Member.
- 3.2 **Delegate** will redirect any complaints/grievances and appeals received verbally or in writing to the **Delegator** within one (1) business day.
- 3.3 **Delegate** will fax all expedited appeals/grievances/complaints immediately upon notification / receipt.

**For Expedited and Standard Appeals and Grievances/Complaints:**

**Medicare:**  
Telephone- 1-800-867-6601 Fax- 1-800-949-2961

**Medicaid:**  
Telephone- 1-800-764-7591 Fax- 1-855-336-6220

**Commercial:**  
Telephone- 1-888-259-6767 Fax- 1-920-339-2112

**Florida Medicaid:**  
Telephone- 1- 800-477-6931 Fax- 1- 800-949-2961

**ARTICLE IV  
TERMINATION**

- 4.1 Notwithstanding anything to the contrary in this UM Attachment, the Addendum, or the Agreement, performance under this UM Attachment may be terminated without cause by either party upon written notice provided to the other party no less than ninety (90) calendar days preceding the termination date or by mutual agreement.
- 4.2 Notwithstanding anything else in this UM Attachment, any breach related to **Delegate’s** accreditation and/or licensure, quality assurance issues or alleged breach regarding termination by **Delegator** in the event **Delegator** determines that **Delegate’s** continued performance of the delegated functions and/or activities under this UM Attachment may affect adversely the health, safety or welfare of any Member or bring **Delegator** or its provider networks in to disrepute, shall be considered non-curable.

- 4.3 If delegated for utilization review and utilization management (UR/UM), the **Delegate** is obligated to send **Delegator** all referrals that have been authorized for dates of service beyond the termination date. This requirement applies to post-service claims and UR/UM delegation.

The Effective Date of this UM Attachment is:                     <Insert Date>                    .

**TABLE 1**  
**Inpatient Utilization Management Functions**

| INPATIENT AND SKILLED NURSING FACILITY ACTIVITIES   | RESPONSIBILITY OF: |          |                         | DETAIL FUNCTION FOR DELEGATOR  | DETAIL FUNCTION FOR DELEGATE   |
|---|--------------------|----------|-------------------------|--|--|
|   | Delegator          | Delegate | Function Not Applicable |  |  |
| <b>INITIAL DETERMINATION</b>  |                    |          |                         |  |  |
| Adoption of UR criteria   | X                  | X        |                         | <b>Delegator</b> reserves the right to approve criteria                                  | For Medicare line of business, the <b>Delegate</b> must apply CMS guidance (Medicare Manual, NCD, LCD, Articles, other); <b>Delegator</b> coverage policy; then Medicare reasonable and necessary criteria. For commercial line of business, UR criteria must be consistent with nationally recognized criteria. <b>Delegate</b> will notify <b>Delegator</b> of its UR criteria annually.   |
| Pre-admission review including determinations of Medical Necessity based on approved criteria, specific group benefits and Member eligibility | X                  | X        |                         | <b>Delegator</b> will perform the function as needed                                     | <b>Delegate</b> will meet established timeframes to complete review for Standard/Non Urgent and Urgent/Expedited requests. <b>Delegate</b> must be available 24 hours a day/365 days, if not, <b>Delegator</b> will perform the function as needed. <u>For Medicare line of business approvals-</u> <b>Delegate</b> may notify Member verbally of approval. If oral notification <b>Delegate</b> must document summary of conversation including date and time. If oral notification is not given, the Member must receive written notification. |
| Monitoring appropriateness, quality and timeliness of decisions of patient services   |                    | X        |                         |  | Compare results of UM activities to predetermined goals. Identify opportunities for improvement and document actions taken.  |
| <b>CONCURRENT REVIEW</b>  |                    |          |                         |  |  |
| On-site or telephonic review for continued stay assessment using approved criteria  |                    | X        |                         |  | <b>Delegate</b> will meet established timeframes to complete review for Standard/Non Urgent and Urgent/Expedited requests.   |
| <b>DISCHARGE PLANNING</b>   |                    |          |                         |  |  |
| Discharge Planning activities from the day of admission until discharge.  |                    | X        |                         |  | Keep <b>Delegator</b> informed of Member's progress if <b>Delegator</b> is responsible for payment of claims.  |
| Case Management (CM)  | X<br>(Market)      | X        |                         | Approve <b>Delegate's</b> CM activities. Communicate to <b>Delegate</b> required reports | <b>Delegate</b> will collaborate with the <b>Delegator's</b> operational team (Health Services Director [HSD]) regarding <b>Delegate's</b> case management activities to prevent duplication of work. <b>Delegate</b> to   |

|   |   |   |  |  |  |
|---|---|---|--|--|--|
|   |   |   |  | and performance standards  | provide reports and performance standards as requested by <b>Delegator</b> .   |
| Arrangement for sub-acute care/outpatient services, i.e. Skilled Nursing Facility (SNF), Home Health, Durable Medical Equipment, and Rehabilitative Services. |   | X |  |  |  |
| Notification to <b>Delegator</b> of last covered day.   |   | X |  |  | Notification to <b>Delegator</b> needs to occur within 24 hours if <b>Delegator</b> is responsible for payment of claims   |
| <b>Delegate</b> will assist with a Member's transition to other care, if necessary, when benefits end.  |   | X |  |  |  |
| <b>RETROSPECTIVE REVIEW</b>   |   |   |  |  |  |
| Review of pended claims for which there were no prior authorizations/reviews.   | X | X |  | <b>Delegator</b> retains final approval rights.  | <b>Delegate</b> will meet established timeframe to complete review and determination.  |
| Review of retrospective authorization requests for which there were no prior authorizations.  | X | X |  | <b>Delegator</b> retains final approval rights.  | <b>Delegate</b> will meet established timeframe to complete review and determination.  |
| <b>REQUIRED NOTIFICATIONS</b>   |   |   |  |  |  |
| Denial determinations   | X | X |  | <b>Delegator</b> retains the right to overturn any denial made by <b>Delegate</b> and will make a determination when there is a lack of agreement between <b>Delegate</b> and referring physician. | <b>Delegate</b> will meet established timeframes to complete review for Standard/Non Urgent and Urgent/Expedited requests.<br><br><b>Delegate</b> to perform and maintain denial log for submission to <b>Delegator</b> as requested |
| Member/legal guardian notification of denial  |   | X |  |  | <b>Delegate</b> will use <b>Delegator</b> approved letter template. <b>Delegate</b> will meet established timeframe to complete review and determination.  |
| Member/legal guardian notification of approval  |   | X |  |  | <b>Delegate</b> will use <b>Delegator</b> approved letter template. <b>Delegate</b> will meet established timeframe to complete review and determination.  |
| Medicare Member/legal guardian verbal   |   | X |  |  |  |

Attachment I.C.1-5 Delegation Services Addendum Delegation

|  |   |   |  |  |  |
|--|---|---|--|--|--|
| notification of denial for expedited request   |   |   |  |  |  |
| Physician/facility notification of denial  |   | X |  |  | <b>Delegate</b> will meet established timeframe to complete review and determination.  |
| Maintenance of Member denial file  |   | X |  |  | <b>Delegate</b> to maintain complete denial file record according to <b>Delegator</b> requirements, including supporting documentation   |
| For Medicare Members: Important Message Notice of Discharge Appeal Rights. (Acute Hospital, LTAC, IRF, and Psychiatric Hospital) |   | X |  |  | Facility responsibility to issue Important Message (IM) with Physician concurrence when planned discharge date is determined. <b>Delegate</b> should assure facility provided Member with IM   |
| For Medicare Members: Notice of Medicare Non Coverage (NOMNC) (Medicare Members in skilled nursing facility (SNF))               |   | X |  |  | Facility or <b>Delegate</b> may issue the NOMNC however the <b>Delegate</b> is ultimately responsible for notice compliance. <b>Delegate</b> is responsible to maintain a log of Members given the NOMNC including those sent to QIO and submit to <b>Delegator</b> as requested along with a copy of the NOMNC (OMB No. 0938-0953)  |
| For Medicare Members: QIO Immediate Review Appeal Notification   | X | X |  | <b>Delegator</b> notifies <b>Delegate</b> Member has appealed hospital discharge | <b>Delegate</b> will be responsible for the following within required timeframes:<br>1. Providing the QIO with supporting documents regarding the current hospital stay<br>2. Issuing to Member and provide a copy to the QIO of the CMS approved Detailed Notice of Discharge OMB No. 0938-1019.<br>3. If requested by the Member, provide the Member any documents provided to the QIO.<br>4. Maintaining a log and file of each occurrence<br>5. Maintaining a copy of each Detailed Notice of Discharge and make available to <b>Delegator</b> , if requested. |

|  |                           |                           |  |  |   |
|--|---------------------------|---------------------------|--|--|---|
| <p>For Medicare Advantage Members: Fast Track Appeal Notification for Skilled Nursing Facility</p> | <p>X</p>                  | <p>X</p>                  |  | <p><b>Delegator</b> notifies <b>Delegate</b> if the QIO contacts <b>Delegator</b> and informs the Plan that the Member has appealed.<br/><b>Delegator</b> notifies <b>Delegate</b> Member has appealed a SNF discharge</p> | <p><b>Delegate</b> will be responsible for the following within required timeframes:</p> <ol style="list-style-type: none"> <li>1. Providing the QIO with supporting documents regarding the current SNF services</li> <li>2. Issuing to the Member and provide a copy to the QIO of the approved Detailed Explanation of Non-Coverage (DENC) OMB 0938-0953.</li> <li>3. If requested by the Member, provide the Member any documents provided to the QIO</li> <li>4. Maintaining a log and file of each occurrence</li> <li>5. Maintaining a copy of each Detailed Explanation of Non-Coverage and make available to <b>Delegator</b>, if requested</li> </ol> |
| <p><b>NETWORK- Contractor to complete. Delete red text prior to executing.</b></p>                 |                           |                           |  |  |   |
| <p>Out of <b>Delegate</b> Network</p>  | <p><b>Option 1:</b> X</p> | <p><b>Option 2:</b> X</p> |  | <p><b>Option 1:</b> <b>Delegator</b> will determine medical necessity for authorization requests for Out-of-Network providers.</p>   | <p><b>Option 2:</b> <b>Delegate</b> will determine medical necessity for authorization requests for Out-of-Network providers.</p>   |
| <p>Out of Service Area</p>   | <p><b>Option 1:</b> X</p> | <p><b>Option 2:</b> X</p> |  | <p><b>Option 1:</b> <b>Delegator</b> will determine medical necessity for authorization requests for Out-of-Service Area providers.</p>  | <p><b>Option 2:</b> <b>Delegate</b> will determine medical necessity for authorization requests for Out-of-Service Area providers.</p>  |

**TABLE 2**  
**Outpatient Utilization Management Functions**

| OUTPATIENT MANAGEMENT ACTIVITIES  | RESPONSIBILITY OF: |          |                         | DETAIL FUNCTION FOR DELEGATOR   | DETAIL FUNCTION FOR DELEGATE  |
|---|--------------------|----------|-------------------------|---|---|
|   | Delegator          | Delegate | Function Not Applicable |   |   |
| <b>INITIAL DETERMINATION</b>  |                    |          |                         |   |   |
| Adoption of UR criteria   | X                  | X        |                         | <b>Delegator</b> reserves the right to approve criteria   | For Medicare line of business, the <b>Delegate</b> must apply CMS guidance (Medicare Manual, NCD, LCD, Articles, other); <b>Delegator</b> coverage policy; then Medicare reasonable and necessary criteria.<br>For commercial line of business, UR criteria must be consistent with nationally recognized criteria.<br><b>Delegate</b> will notify <b>Delegator</b> of its UR criteria annually.  |
| Determine the appropriateness of each referral to specialists, etc. for Medical Necessity. For Medicare Members the <b>Delegate</b> must accept written and verbal requests |                    | X        |                         |   | <b>Delegate</b> to perform and monitor referral process for Standard/Non Urgent and Urgent/Expedited.<br><b>Delegate</b> will meet established timeframe to complete review and notify the provider and Member of the determinations.<br><u>For Medicare line of business approvals-</u> <b>Delegate</b> must notify Member verbally of approval and document brief summary of conversation including date and time. If the Member is unavailable then a written notification must be sent to the Member. |
| Case Management (CM)  | X<br>(Market)      | X        |                         | Approve <b>Delegate's</b> CM activities. Communicate to <b>Delegate</b> required reports and performance standards. | <b>Delegate</b> will collaborate with the <b>Delegator's</b> operational team (HSD) regarding <b>Delegate's</b> case management activities (Short term case management and transition of care) to prevent duplication of work. <b>Delegate</b> to provide reports and performance standards as requested by <b>Delegator</b> .  |
| Member Communications   |                    | X        |                         |   | The <b>Delegate</b> will provide eligible Members the following written information about the program:<br>1. how to use the services;   |

|   |   |   |  |   |  |
|---|---|---|--|---|--|
|   |   |   |  |   | 2. how Members become eligible to participate; and<br>3. how to opt in our opt out.  |
| Monitoring appropriateness, quality and timeliness of decisions of patient services                   |   | X |  |   | Compare results of UM activities to predetermined goals. Identify opportunities for improvement and document actions taken.  |
| <b>Delegate</b> will assist with a Member's transition to other care, if necessary, when benefits end |   | X |  |   |  |
| <b>RETROSPECTIVE REVIEW</b>   |   |   |  |   |  |
| Review of pended claims for which there were no prior authorizations/reviews                          | X | X |  | <b>Delegator</b> retains final approval rights  | <b>Delegate</b> will meet established timeframe to complete review and determination.  |
| Review of retrospective authorization requests for which there were no prior authorizations           | X | X |  | <b>Delegator</b> retains final approval rights  | <b>Delegate</b> will meet established timeframe to complete review and determination.  |
| <b>REQUIRED NOTIFICATIONS</b>   |   |   |  |   |  |
| Denial determination  | X | X |  | <b>Delegator</b> retains the right to overturn any denial made by <b>Delegate</b> and will make determination when there is lack of agreement between <b>Delegate</b> and referring physician | <b>Delegate</b> will meet established timeframes to complete review for Standard/Non Urgent and Urgent/Expedited requests.   |
| Member/legal guardian denial notification   |   | X |  |   | <b>Delegate</b> will use <b>Delegator</b> approved letter template. <b>Delegate</b> will meet established timeframe.   |
| Member/legal guardian approval notification   |   | X |  |   | <b>Delegate</b> will use <b>Delegator</b> approved letter template. <b>Delegate</b> will meet established timeframe.   |
| Physician/Facility notification   |   | X |  |   | <b>Delegate</b> will meet established timeframe.   |
| Member/guardian verbal notification of denial for expedited request                                   |   | X |  |   | <b>Delegate</b> will meet established timeframe.   |
| Maintenance of Member denial file   |   | X |  |   | <b>Delegate</b> to maintain complete denial file record according to <b>Delegator</b> requirements, including all supporting documentation specified by <b>Delegator</b> . |

|  |          |          |  |   |   |
|--|----------|----------|--|---|---|
| <p>For Medicare Members: Notice of Medicare Non Coverage (NOMNC) (Medicare Members in home health agency (HHA), or comprehensive outpatient rehabilitation facility (CORF)</p> |          | <p>X</p> |  |   | <p>Facility or <b>Delegate</b> may issue the NOMNC however the <b>Delegate</b> is ultimately responsible for notice compliance. <b>Delegate</b> is responsible to maintain a log of Members given the NOMNC including those sent to QIO and submit to <b>Delegator</b> as requested along with a copy of the NOMNC (OMB No. 0938-0953)</p>  |
| <p>For Medicare Advantage Members: Fast Track Appeal Notification- DENC Home Health Agency (HHA), or Comprehensive Outpatient Rehabilitation Facility (CORF)</p>               | <p>X</p> | <p>X</p> |  | <p><b>Delegator</b> notifies <b>Delegate</b> if the QIO contacts <b>Delegator</b> and informs the Plan that the Member has appealed. <b>Delegator</b> notifies <b>Delegate</b> Member has appealed HHA or CORF discharge.</p> | <p><b>Delegate</b> will be responsible for the following within required timeframes:</p> <ol style="list-style-type: none"> <li>1. Providing the QIO with supporting documents regarding the current services.</li> <li>2. Issuing to the Member and provide a copy to the QIO of the approved Detailed Explanation of Non-Coverage (DENC) OMB 0938-0953. If requested by the Member, provide the Member any documents provided to the QIO.</li> <li>4. Maintaining a log and file of each occurrence</li> <li>5. Maintaining a copy of each Detailed Explanation of Non-Coverage and make available to <b>Delegator</b>, if requested</li> </ol> |
| <b>ADDITIONAL INPATIENT/OUTPATIENT ACTIVITIES</b>  |          |          |  |   |   |
| <p>Identification and notification of any potential quality of care concerns.</p>  |          | <p>X</p> |  |   | <p><b>Delegate</b> to notify <b>Delegator</b> of any potential quality of care concerns.</p> <ol style="list-style-type: none"> <li>1. Contact <b>Delegator's</b> Quality Director to confirm email and fax number.</li> <li>2. Complete <b>Delegator's</b> referral form QM-061.</li> <li>3. Submit completed referral form to <b>Delegator</b> within two (2) business days of identification of potential quality of care concern.</li> <li>4. Member quality of care complaints, received verbally or in writing, are considered grievances and <b>Delegate</b> shall handle in accordance with Section 3.1 of this UM Attachment.</li> </ol> |

|   |                    |                    |  |   |  |
|---|--------------------|--------------------|--|---|--|
| Quality of care concerns  | X                  |                    |  | <b>Delegator</b> does not delegate the investigation of quality of care concerns. | <b>Delegate</b> to notify <b>Delegator</b> of any quality of care concerns.<br><b>Delegate</b> to notify <b>Delegator</b> .<br>1. Contact <b>Delegator's</b> Quality Director to confirm email and fax number.<br>2. Complete <b>Delegator's</b> referral form QM-061.<br>3. Submit completed referral form to <b>Delegator</b> within two (2) business days of identification of potential quality of care concern.<br>4. Member quality of care complaints, received verbally or in writing, are considered grievances and <b>Delegate</b> shall handle in accordance with Section 3.1 of this UM Attachment.    |
| I.D. and notification of critical incidents and or sentinel events and hospital reportable incidents regarding Member services  |                    | X                  |  |   | <b>Delegate</b> to notify <b>Delegator</b> of any critical incidents and or sentinel events and hospital reportable incidents.<br>1. Contact <b>Delegator's</b> Quality Director to confirm email and fax number.<br>2. Complete <b>Delegator's</b> referral form QM-061.<br>3. Submit completed referral form to <b>Delegator</b> within two (2) business days of identification of potential quality of care concern.<br>4. Member quality of care complaints, received verbally or in writing, are considered grievances and <b>Delegate</b> shall handle in accordance with Section 3.1 of this UM Attachment. |
| Primary Care Physician (PCP) termination Member notification<br><b>(Contractor to select one option based on selection made above. Delete this message and delete non-applicable option.)</b> | <b>Option 1:</b> X | <b>Option 2:</b> X |  | <b>Option 1:</b> <b>Delegator</b> will notify Member.                             | <b>Option 2:</b> <b>Delegate</b> must notify <b>Delegator</b> of all PCP terminations.   |
| Specialist termination Member notification  | <b>Option 1:</b> X | <b>Option 2:</b>   |  | <b>Option 1:</b> <b>Delegator</b> will notify Member.                             | <b>Option 2:</b> <b>Delegate</b> will utilize <b>Delegator's</b> Member notification letter template.  |

|   |                    |                    |  |  |  |
|---|--------------------|--------------------|--|--|--|
| (Contractor to select one option based on selection made above. Delete this message and delete non-applicable option.)  |                    | X                  |  |  |  |
| Allowance of Member continued access to a provider when that provider's contract is discontinued (for reasons other than cause)(Contractor to fill in who will manage this process. Party that determines COC is responsible for notification of COC to members.) | <b>Option 1:</b> X | <b>Option 2:</b> X |  | <b>Option 1:</b> Delegator will determine COC.                         | <b>Option 2:</b> The Delegate will determine COC. The <b>Delegate</b> will be expected to provide the following:<br>1. Continuation of treatment through the lesser of the current period of active treatment, or for up to 90 calendar days for Members undergoing active treatment for a chronic or acute medical condition.<br>2. Additional requirements will be according to state regulations. |
| Operation Implementation  | X                  | X                  |  | <b>Delegator</b> will provide <b>Delegate</b> with required procedures | During the operations implementation phase, the <b>Delegate</b> will be informed of procedures that will need to be implemented by the <b>Delegate</b> in regards to the functions that are or are not delegated.  |
| Provider over/underutilization of services  |                    | X                  |  |  | <b>Delegate</b> agrees to have a mechanism in place to detect both over/underutilization of services   |
| Member satisfaction with the UM process   | X                  |                    |  |  |  |
| Reporting fraud and abuse information identified through the UM program   |                    | X                  |  |  | <b>Delegate</b> shall report any findings to <b>Delegator</b> upon discovery.  |
| Practitioner satisfaction with the UM process   | X                  | X                  |  | <b>Delegator</b> will review <b>Delegate's</b> results                 | <b>Delegate</b> will collect and complete an initial analysis of the data and identify opportunities for improvement   |
| Establishing, applying and maintaining pharmaceutical management procedures   | X                  |                    |  |  |  |
| Evaluating new technology   | X                  |                    |  | Evaluating new technology  |  |
| Transplant Services UM/UR and Case Management (CM) for transplant services  | X                  | X                  |  | <b>Delegator</b> does not delegate Transplant Services                 | <b>Delegate</b> will notify the <b>Delegator</b> Transplant department immediately upon identification of a potential or requested transplant evaluation@ 1-866- 421-5663,   |

|   |                    |                    |  |   |   |
|---|--------------------|--------------------|--|---|---|
|   |                    |                    |  |   | Fax: 502 508 9300, email: Transplant@humana.com<br><b>Delegate</b> shall assist in clarification of admission and discharge dates of transplant related admissions. |
| Member communication  |                    | X                  |  |   | <b>Delegate</b> should communicate with Members regarding the UM process and authorization of care  |
| Managing triage and referral of behavioral healthcare                       | X                  | X                  |  | Instructions are available in the Member and Provider Handbook  | <b>Delegate</b> agrees to support downstream entities through education of established processes  |
| Provision of Member experience data   | X                  |                    |  | <b>Delegator</b> to provide data upon <b>Delegate's</b> request   |   |
| Provision of clinical performance data                                      |                    | X                  |  |   |   |
| <b>NETWORK- Contractor to complete. Delete red text prior to executing.</b> |                    |                    |  |   |   |
| Out of <b>Delegate</b> Network  | <b>Option 1:</b> X | <b>Option 2:</b> X |  | <b>Option 1: Delegator</b> will determine medical necessity for authorization requests for Out-of-Network providers.      | <b>Option 2: Delegate</b> will determine medical necessity for authorization requests for Out-of-Network providers.   |
| Out of Service Area   | <b>Option 1:</b> X | <b>Option 2:</b> X |  | <b>Option 1: Delegator</b> will determine medical necessity for authorization requests for Out-of-Service Area providers. | <b>Option 2: Delegate</b> will determine medical necessity for authorization requests for Out-of-Service Area providers.  |

**TABLE 3**  
**REQUIRED UTILIZATION MANAGEMENT REPORTS**

**All reports are to be sent using the secured email procedure and sent to your assigned delegation compliance consultant.**

| MANDATORY REPORTS  | FREQUENCY                        | DETAIL   |
|--|----------------------------------|--|
| <b>The below reporting requirements apply to outpatient and inpatient delegated functions.</b>   |                                  |  |
| Total number of processed referrals to include DME and Home Health. The number of UM cases handled by type: Pre-service; Urgent; Concurrent; Post- service for inpatient and or outpatient services. Total number of approved and denied cases | Quarterly                        |  |
| Referral log   | Quarterly                        | To include analysis of compliance with meeting turn-around timeframes  |
| Denial log   | Quarterly                        | Refer to case log data documentation requirements.   |
| Initial Urgent/Expedited Determination log   | Quarterly                        | Refer to case log data documentation requirements.   |
| CMS Required Medicare Part C – Organizational Determinations   | Quarterly                        | <b>This must be reported 15 days following the end of the quarter</b>  |
| MA Appeal Rights fast-track appeal log   | Quarterly                        |  |
| ER visits that do not result in inpatient visit per thousand   | Quarterly                        |  |
| Case Management Activities   | As requested by <b>Delegator</b> | Report requirements and performance standards will be provided to the <b>Delegate</b> by the Health Services Director (HSD)<br><b>Delegate</b> shall notify the HSD Director or designee prior to any changes to the CM activities for approval. |
| UM Program   | Annually                         |  |
| UM Work plan   | Annually                         |  |
| Previous year UM Program Evaluation  | Annually                         |  |
| UM Policies and Procedures   | Annually                         |  |
| UM Medical Review Criteria to be used in the forthcoming year  | Annually                         |  |
| Risk Management issues   | Concurrently                     |  |
| Physician Satisfaction with the UM management process  | Annually                         |  |
| <b>The below reporting requirements apply to inpatient delegated functions.</b>  |                                  |  |
| Acute Inpatient and Calculated Monthly<br>1) Admits/1000<br>2) Days/1000<br>3) Average Length of Stay<br>4) Readmission rate within 30 days<br>5) Number of inpatient stay denials   | Quarterly                        |  |
| Inpatient Detailed Notice of Discharge log and copy of notice sent to the Member   | Quarterly                        |  |

| MANDATORY REPORTS   | FREQUENCY | DETAIL |
|---|-----------|--------|
| LTACH - Calculated Monthly <ul style="list-style-type: none"> <li>• Admits/1000</li> <li>• Days/1000</li> <li>• Average Length of Stay</li> <li>• Readmission rate within 30 days</li> <li>5. Number of LTACH stay denials</li> </ul>   | Quarterly |        |
| SNF - Calculated Monthly <ol style="list-style-type: none"> <li>1) Admits/1000</li> <li>2) Days/1000</li> <li>3) Average Length of Stay</li> <li>4) Readmission rate within 30 days</li> <li>5) Number of SNF stay denials</li> </ol>   | Quarterly |        |
| Log for SNF/HHC and CORF appeals with copies of the Detailed Explanation of Coverage letters given to Members   | Quarterly |        |
| Rehab - Calculated Monthly <ul style="list-style-type: none"> <li>• Admits/1000</li> <li>• Days/1000</li> <li>• Average Length of Stay</li> <li>• Readmission rate within 30 days</li> <li>5. Number of Rehab stay denials</li> </ul>   | Quarterly |        |
| Note: Reporting requirements may change based upon revised or new state and federal legislation, NCQA standards and <b>Delegator</b> requirements during the term of this UM Attachment.  |           |        |
| All reports and subsections of reports must be LOB and <b>Delegator</b> market specific. The analysis of data and identified opportunities for improvement must include documentation of interventions implemented. Outcomes and/or status should be documented in the next scheduled report. <b>Reporting formats must be pre-approved by Delegator.</b> |           |        |
| <b>Quarterly</b> – 60 days following the end of the quarter<br><b>Annually</b> – March 15   |           |        |

**TABLE 4**  
**CASE LOG DATA REQUIREMENTS**

| DATA ELEMENTS   | STANDARD DENIAL LOG | EXPEDITED DENIAL LOG | URGENT DENIAL LOG | STANDARD AUTH LOG | EXPEDITED AUTH LOG | URGENT AUTH LOG |
|---|---------------------|----------------------|-------------------|-------------------|--------------------|-----------------|
| Line of business  | X                   | X                    | X                 | X                 | X                  | X               |
| Member Identification number  | X                   | X                    | X                 | X                 | X                  | X               |
| Member name   | X                   | X                    | X                 | X                 | X                  | X               |
| Type of Service Inpatient/Outpatient  | X                   | X                    | X                 | X                 | X                  | X               |
| Priority of request Standard/Expedited/Urgent   | X                   | X                    | X                 | X                 | X                  | X               |
| Facility/physician name   | X                   | X                    | X                 | X                 | X                  | X               |
| Date of receipt of request for services   | X                   | X                    | X                 | X                 | X                  | X               |
| Time of receipt of request for services   |                     | X                    |                   |                   | X                  |                 |
| Date additional information requested   | X                   | X                    | X                 | X                 | X                  | X               |
| Date additional information received  | X                   | X                    | X                 | X                 | X                  | X               |
| Decision date   | X                   | X                    | X                 | X                 | X                  | X               |
| Time of verbal notification to the Member   |                     | X                    |                   |                   | X                  |                 |
| Date letter delivered or sent to Member   | X                   | X                    | X                 |                   |                    | X               |
| Date PCP/referring practitioner notified  | X                   | X                    | X                 | X                 | X                  | X               |
| Date of denial recommendation to <b>Delegator</b> , if applicable   |                     |                      |                   |                   |                    |                 |
| Type of denial  | X                   | X                    | X                 |                   |                    |                 |
| Reason for denial   | X                   | X                    | X                 |                   |                    |                 |
| Last Covered Day date, if applicable  | X                   | X                    | X                 | X                 | X                  | X               |
| MD Reviewer   | X                   | X                    | X                 |                   |                    |                 |
| Analysis and summary of compliance to timeliness standards including percent of compliance meeting timeliness standards | X                   | X                    | X                 | X                 | X                  | X               |

**TABLE 5  
FILE REQUIREMENTS**

| INFORMATION MAINTAINED   | STANDARD DENIAL FILE | EXPEDITED DENIAL FILE | URGENT DENIAL FILE | STANDARD AUTH FILE | EXPEDITED AUTH FILE | URGENT AUTH FILE |
|--|----------------------|-----------------------|--------------------|--------------------|---------------------|------------------|
| Member name  | X                    | X                     | X                  | X                  | X                   | X                |
| Member identification number   | X                    | X                     | X                  | X                  | X                   | X                |
| Type of service requested<br>Inpatient/Outpatient  | X                    | X                     | X                  | X                  | X                   | X                |
| Priority of Request<br>Standard/Expedited/Urgent   | X                    | X                     | X                  | X                  | X                   | X                |
| Date request for services received   | X                    | X                     | X                  | X                  | X                   | X                |
| Time request for services received   |                      | X                     |                    |                    | X                   |                  |
| Date additional information requested  | X                    | X                     | X                  | X                  | X                   | X                |
| Date additional information received   | X                    | X                     | X                  | X                  | X                   | X                |
| Decision date  | X                    | X                     | X                  | X                  | X                   | X                |
| Date written notification provided to Member and referring physician   | X                    | X                     | X                  | X                  | X                   | X                |
| Time written notification provided to Member and referring physician   | X                    | X                     |                    |                    | X                   |                  |
| Date verbal notification provided to Member and referring physician  | X                    | X                     | X                  |                    | X                   | X                |
| Time verbal notification provided to Member and referring physician  |                      | X                     |                    |                    | X                   |                  |
| Copy of denial letter  | X                    | X                     | X                  |                    |                     |                  |
| Copy of approval letter  |                      |                       |                    | X                  | X                   | X                |
| Signature of physician reviewer for Commercial line of business  | X                    | X                     | X                  |                    |                     |                  |
| Clinical rationale/criteria  | X                    | X                     | X                  |                    |                     |                  |
| Peer to peer <ul style="list-style-type: none"> <li>• Documentation the requesting physician had the opportunity to discuss the case with the physician reviewer. Must be able to demonstrate reasonable opportunity and provide documentation of physician contact, date and time.</li> </ul> | X                    | X                     | X                  |                    |                     |                  |
| Supporting medical documentation   | X                    | X                     | X                  |                    |                     |                  |

**TABLE 6  
REQUIRED BEHAVIORAL HEALTH UTILIZATION MANAGEMENT REPORTS**

**CONTRACTORS REMOVE THIS PAGE IF THERE IS NO BH DELEGATION**

| MANDATORY REPORTS   | FREQUENCY     | DETAIL                                 |
|---|---------------|--|
| Behavioral Health (BH) Quality of Care/Sentinel Event Report (as reported to <b>Delegator</b> )   | Quarterly     |  |
| BH Accessibility Report - Total number of new referrals for Emergent, Urgent & Routine cases. Analysis of compliance with meeting turn-around timeframes. Report should include the turn-around times between the Member's referral and the Member's start date for new episodes of care.   | Quarterly     |  |
| Encounter data for behavioral health admissions and ambulatory services that includes (Member ID, Member name, DOB, date of service, CPT code, Provider or Facility Name, Provider ID, Provider type, address, phone number and place of service.   | Quarterly     | <b>Delegate will assist Delegator.</b> |
| HEDIS Behavioral Health Activity Report for Follow-up after Hospitalization (FUH) for Mental Illness: AMM - Anti-Depressant Medication Management, IET - Initiation and Engagement of Alcohol and other Drug Dependence treatment. (as applicable – based on <b>Delegator's</b> annual report)  | Semi-Annually | <b>Delegate will assist Delegator.</b> |
| Approval of additional behavioral health clinical practice guidelines   | Annually      |  |
| Note: Reporting requirements may change based upon revised or new state and federal legislation and NCQA standards requirements during the term of this UM Attachment.  |               |  |
| All reports and subsections of reports must be LOB and <b>Delegator</b> market specific. The analysis of data and identified opportunities for improvement must include documentation of interventions implemented. Outcomes and/or status should be documented in the next scheduled report. <b>Reporting formats must be pre-approved by Delegator.</b> |               |  |
| <p align="center"><b>Monthly</b> – 30 days following the end of the month<br/> <b>Quarterly</b> – 60 days following the end of the quarter<br/> <b>Annually</b> – March 15</p>  |               |  |

## DELEGATION OF COMPLEX CASE MANAGEMENT ATTACHMENT

This **Delegation of Complex Case Management Attachment** (“CCM Attachment”) is hereby made part of and incorporated into the Agreement and the Delegation Services Addendum, entered into between **<Insert Name of the Delegator Humana > (Delegator)**, and **<Insert Name> (Delegate)**. This CCM Attachment is intended to amend the terms and conditions of the Addendum and to the extent that this CCM Attachment conflicts with the terms and conditions of the Agreement or the Addendum, including any prior agreements, addenda, exhibits, or attachments, this CCM Attachment controls the relationship between the parties.

### ARTICLE I DELEGATE’S OBLIGATIONS

**Delegate** agrees that it shall:

- 1.1 Acknowledge and agree that **Delegate’s** policies and procedures are subject to **Delegator’s** review and written approval prior to any delegation of Complex Case Management (CCM) functions.
- 1.2 Accept the responsibility and the obligation for performing all CCM delegated functions and activities specified in **TABLE 1**, which is attached hereto and incorporated by reference herein, as they relate to services rendered to Members assigned to physicians, employees, Subcontractors and independent contractors.
- 1.3 Acknowledges and agrees that clinical assessments of Members are required to be performed by licensed registered nurses (RN) in accordance with nurse practice guidelines and licensure requirements.
- 1.4 Comply with **Delegator’s** policies, procedures, and program requirements and all applicable state and federal laws, rules and regulations and Accreditation Organization requirements pertaining to CCM and the delivery of medical and related health care services.
- 1.5 Demonstrate **Delegate’s** CCM program plan, previous plan evaluation, and subsequent revisions have been approved by **Delegate’s** internal quality/utilization management (UM) committee.
- 1.6 Not provide incentives to deny, limit, or discontinue Medically Necessary services. Nothing contained in this CCM Attachment or the Agreement is intended by **Delegator** to be a financial incentive or payment, which directly or indirectly acts as an inducement for the **Delegate** to limit Medically Necessary services.
- 1.7 Retain all Member-related information and records created for a period of not less than ten (10) years.
- 1.8 Acknowledge that **Delegator** retains all other CCM functions not specified as the **Delegate’s** responsibility in this CCM Attachment.

### ARTICLE II ACCESS, AUDIT, AND OVERSIGHT

**Delegate** agrees that it shall:

- 2.1 At least annually, or more frequently if deemed necessary by **Delegator**, and then upon not less than ten (10) business days prior notice, or such shorter notice as may be imposed on **Delegator** by a federal or state regulatory agency or Accreditation Organization, allow **Delegator**, its designee, and any state or federal entity or Accreditation Organization to access all CCM documentation, processes, policies, systems, and files in order to perform an audit review of the **Delegate’s** policies and procedures, program plan, QI/UM Committee meeting minutes that have been approved by the **Delegate’s** QI/UM Committee, and **Delegate’s** performance/compliance under this CCM Attachment. In-person or telephonic/virtual meetings with participation of both **Delegator** and the **Delegate** will be held to discuss results of audits or reports on an as needed basis.

- 2.2 Submit to **Delegator**, with respect to delegated functions, all required reports and analyses, as indicated in **TABLE 2**, which is attached and hereby incorporated by reference, along with identified problems, corrective actions initiated, and outcomes.
  - a. All reports and subsections of reports must be specific to line of business and offering **Delegator's** affiliate, and all reporting formats must be pre-approved by **Delegator**.
  - b. The analysis of data must address identified opportunities for improvement with dates that documented interventions were implemented. The next scheduled report must address follow up activities, outcomes and/or status.
  - c. **Delegate** agrees to provide any and all reports requested by **Delegator** within timeframes identified by **Delegator** to ensure **Delegator** meets all new and revised **Delegator**, CMS, Federal, State and Accreditation Organization reporting requirements.
- 2.3 Acknowledge and agree that **Delegator** maintains the ultimate responsibility for the sufficiency and appropriateness of the DM programs and retains the right to implement a Corrective Action Plan (CAP), suspend or terminate any of this CCM Attachment at any time **Delegate** fails to meet or comply with **Delegator's** policies, procedures, and program requirements and all applicable state and federal laws, rules and regulations and Accreditation Organization requirements.
- 2.4 Should the **Delegate** be placed on a CAP, the **Delegate** will have fourteen (14) calendar days to provide a written response describing how they will meet the requirements found to be noncompliant including prospective date of compliance.
- 2.5 **Delegate** will be subject to a capitation payment penalty as indicated in the table below for any outstanding issues noted on a CAP:

| <b>Outstanding Corrective Action Plan</b> | <b>0 to 3 months</b> | <b>4-6 months</b>                      | <b>7-9 months</b>                      | <b>10-12 months or greater</b>         |
|---|----------------------|--|--|--|
| <b>Payment Penalty</b>                    | <b>0%</b>            | <b>1% per month until CAP resolved</b> | <b>2% per month until CAP resolved</b> | <b>3% per month until CAP resolved</b> |

**ARTICLE III  
MEMBER APPEALS AND GRIEVANCES/COMPLAINTS**

- 3.1 **Delegator's** Member expedited and standard complaints/appeals/grievances are not delegated. **Delegator** maintains all Member rights and responsibility functions. **Delegator** will handle all Member appeals/ grievances/complaints for denied services including expedited and standard complaints/appeals/grievances made by a physician/practitioner on behalf of the Member
- 3.2 **Delegate** will redirect any complaint/grievance and appeal received verbally or in writing to the **Delegator** within one (1) Business Day.
- 3.3 **Delegate** will fax all expedited appeals/grievances/complaints to **Delegator** immediately upon notification/receipt.

**For Expedited and Standard Member Appeals and Grievances/Complaints:**

**Medicare:**  
Telephone- 1-800-867-6601      Fax- 1-800-949-2961

**Medicaid:**  
Telephone- 1-800-764-7591      Fax- 1-855-336-6220

**Commercial:**

Telephone- 1-888-259-6767 Fax- 1-920-339-2112

**FL Medicaid only:**

Telephone- 1-800-477-6931 Fax- 1-800-949-2961

**ARTICLE IV  
TERMINATION**

- 4.1 Notwithstanding anything to the contrary in this CCM Attachment, the Addendum, or the Agreement, performance under this CCM Attachment may be terminated without cause by either party upon written notice provided to the other party no less than ninety (90) calendar days preceding the termination date or by mutual agreement.
- 4.2 Notwithstanding anything else in this CCM Attachment, any breach related to **Delegate's** accreditation and/or licensure, quality assurance issues or alleged breach regarding termination by **Delegator** in the event **Delegator** determines that **Delegate's** continued performance of the delegated functions and/or activities under this CCM Attachment may affect adversely the health, safety or welfare of any Member or bring **Delegator** or its provider networks in to disrepute, shall be considered non-curable.

The **Effective Date** of this CCM Attachment is:                     <Insert Date>

**TABLE 1  
COMPLEX CASE MANAGEMENT FUNCTIONS**

| COMPLEX CASE MANAGEMENT ACTIVITIES        | DETAIL FUNCTION FOR DELEGATOR   | DETAIL FUNCTION FOR DELEGATE  |
|---|---|---|
| Population Assessment                     |   | <p>Annually assesses the characteristics and needs of its member population and relevant subpopulations as indicated. This would include assessing the needs of children, adolescents, individuals with physical or developmental disabilities and individuals with serious and persistent mental illness.</p> <p>Annually reviews and updates CCM processes and resources if necessary to meet member needs.</p> <p>Note: Assessment of needs of children and adolescents is not applicable for Medicare only line of business.</p>  |
| Program Description                       |   | <p>The organization's CCM program description has policies and procedures for identification of patients and assessment of patient need. The program description includes evidence on which the program is based; criteria for identifying eligible patients; services offered, program goals and how case management services are integrated with the services or others involved in the Member's care.</p> <p>Annually measures the effectiveness of its CCM program.</p>   |
| Identification of Members                 | <p><b>Delegator</b> will assist <b>Delegate</b> in providing reporting data as requested by <b>Delegate</b></p> | <p>The <b>Delegate's</b> policy should identify the CCM enrollment criteria and contain a list of data sources used such as claims or encounter data, hospital discharge data, pharmacy data (if applicable) and purchaser data (if applicable), UM data such as precertification or hospital admission data, DM program referral, discharge planner referral, UM referral, Member or care giver self-referral, practitioner referral and a behavioral health referral.</p>   |
| Access to CCM                             |   | <p>The <b>Delegate's</b> policy should identify multiple avenues for Members to be considered for CCM services including referrals from a health information line, DM program, discharge planner, UM, Member or caregiver, and practitioner referral.</p>   |
| Case management (CM) systems              |   | <p><b>Delegate</b> will use a CM system with: 1. Evidence-based clinical guidelines or algorithms to conduct assessment and management, 2. Documentation of staff Member's ID, date and time of each case activity including interaction with the Member and 3. Prompts for follow up.</p>  |
| Member Communications                     |   | <p>The <b>Delegate</b> will provide eligible Members the following written information about the program:</p> <ol style="list-style-type: none"> <li>1. how to use the services;</li> <li>2. how Members become eligible to participate; and</li> <li>3. how to opt in or opt out.</li> </ol>   |
| Case management process and documentation |   | <p><b>Delegate's</b> policies should include the process to assess the needs of each member requiring CCM for developing an effective CM plan and must address how <b>Delegate</b> maintains CM notes that describe the assessment results for each factor. The following factors need to be addressed:</p> <ol style="list-style-type: none"> <li>1. documentation of clinical history including medications;</li> <li>2. initial assessment of Member's health status including condition-specific issues, activities of daily living, behavioral health status including cognitive functions, psychosocial issues and life-planning activities;</li> <li>3. evaluation of cultural and linguistic needs, preferences or limitations, visual and hearing needs, preferences or limitations, caregiver resources and involvement, available benefits and community resources;</li> </ol> |

| COMPLEX CASE MANAGEMENT ACTIVITIES  | DETAIL FUNCTION FOR DELEGATOR                                   | DETAIL FUNCTION FOR DELEGATE   |
|---|---|--|
|   |   | <p>4. development of an individualized case management plan, including prioritized goals considering the Member’s and caregiver’s goals, preferences and desired level of involvement in the CM plan, a schedule for follow-up and communication with Members and communication of Member self-management plans;</p> <p>5. identification of barriers to a Member meeting goals or complying with the plan;</p> <p>6. facilitation of Member referrals to resources and follow-up process to determine whether Members act on referrals;</p> <p>7. a process to assess Member’s progress against CM plans for Members; and</p> <p>8. determining when follow up is not appropriate.</p> <p>The initial assessment must be completed within thirty (30) calendar days from the date the Member is determined to be eligible for CCM.</p>  |
| Appropriate policies and procedures                                       |   | <p><b>Delegate</b> must have documented policies and procedures that meet National Committee for Quality Assurance (NCQA) and Centers for Medicare and Medicaid Services (CMS) requirements, as applicable.</p>  |
| Maintenance of complete CCM files   |   | <p>At least annually and as requested by <b>Delegator</b>, the <b>Delegate</b> will produce CCM files selected by <b>Delegator</b>. Refer to TABLE 3 for required CCM file content. For <b>Delegator</b> auditing purposes files of eligible Members may be excluded when 3 or more attempts to reach the Member are made in a 2 week period within the initial thirty (30) calendar days.</p>   |
| Member experience with case management                                    | Approve Member satisfaction survey prior to <b>Delegate</b> use | <p>The <b>Delegate</b> will perform a Member satisfaction survey with the CCM Program at least annually and provides the results with analysis and improvement activities to <b>Delegator</b>. The survey must be approved by <b>Delegator</b>.</p> <p>The <b>Delegate</b> will analyze Member feedback considering quantitative and qualitative data to identify patterns and opportunities to improve satisfaction with its CCM program.</p> <p>The survey should cover, at a minimum:</p> <ol style="list-style-type: none"> <li>1. information about the overall program;</li> <li>2. the program staff;</li> <li>3. usefulness of the information disseminated; and</li> <li>4. Member’s ability to adhere to recommendations.</li> </ol>   |
| Measure effectiveness, action taken and re-measurement of the CCM Program |   | <p>Annually, the <b>Delegate</b> will measure the effectiveness of its CCM Program using three measures. For each measure the <b>Delegate</b>:</p> <ol style="list-style-type: none"> <li>1. identifies a relevant process or outcome;</li> <li>2. uses valid methods that provide quantitative results;</li> <li>3. sets a performance goal;</li> <li>4. clearly identifies measure specifications;</li> <li>5. collects data and analyzes results; and</li> <li>6. identifies opportunities for improvement, if applicable.</li> </ol> <p>Based upon the results of the effectiveness and satisfaction of the CCM program, if applicable, the <b>Delegate</b> implements at least one intervention to improve clinical performance and to improve Member satisfaction. In addition, if applicable, the <b>Delegate</b> should re-measure to determine the impact on clinical performance and or the Member experience.</p> |

**TABLE 2  
REQUIRED COMPLEX CASE MANAGEMENT REPORTS**

**All reports are to be sent using the secured email procedure and sent to your assigned delegation compliance consultant.**

| MANDATORY REPORTS  | FREQUENCY                           | DETAIL  |
|--|-------------------------------------|---|
| <b>Delegate</b> will submit a CCM log to <b>Delegator</b> in the format listed on <b>Table 3</b>   | Quarterly<br>Biannually as directed |   |
| Reporting of <b>Delegate's</b> CCM program analysis of effectiveness using aggregated quarterly report data.   | Annually                            |   |
| Report CCM program active Member participation rates   | Quarterly<br>Annually               |   |
| CCM Annual Program   | Annually                            |   |
| Previous year CCM Programs effectiveness evaluation  | Annually                            | Measure the CCM program's effectiveness and satisfaction. If applicable:<br>1. implement at least one intervention to improve clinical performance<br>2. implement at least one intervention to improve Member satisfaction<br>3. perform re-measures to determine the impacts on clinical performance and the member experience. |
| Member CCM Program Satisfaction Survey   | Annually                            | Determine performance goals for the Member satisfactory survey and conduct a causal analysis if stated goals were not met.  |
| Analysis of Member complaints specific to CCM program-all other complaints must be sent directly to <b>Delegator</b>   | Annually                            | <b>Delegate</b> shall analyze complaints to identify opportunities to improve satisfaction with its complex case management program.  |
| <b>Delegator</b> will provide <b>Delegate</b> Member experience and clinical performance data if applicable.   | As requested                        |   |
| Identification of Members eligible for Complex Case Management using identified data sources.  | Quarterly                           |   |
| <p align="center">Note: Reporting requirements may change based upon revised or new state and federal legislation, <b>Delegator</b> and NCQA standards requirements during the term of this Attachment.</p> <p align="center">All reports and subsections of reports must be LOB and <b>Delegator</b> market specific.<br/>The analysis of data and identified opportunities for improvement must include documentation of interventions implemented. Outcomes and/or status should be documented in the next scheduled report.<br/><b>Reporting formats must be pre-approved by Delegator.</b></p> <p align="center"><b>Monthly</b> – 30 days following the end of the month<br/><b>Quarterly</b> – 60 days following the end of the quarter<br/><b>Annually</b> – March 15</p> |                                     |   |

**TABLE 3  
DOCUMENTATION REQUIREMENTS**

| <b>Documentation Required</b>   | <b>CCM File</b> | <b>CCM Log</b> |
|---|-----------------|----------------|
| Line of business  | X               | X              |
| Member Identification number  | X               | X              |
| Member name   | X               | X              |
| Primary Care Physician name   | X               |                |
| Names of all involved healthcare professionals including contact information  | X               |                |
| Date enrolled in CCM  | X               | X              |
| Member diagnoses  | X               | X              |
| Location of member- i.e. home, facility(include address)  | X               |                |
| Initial assessment of Member health status, including condition-specific issues   | X               |                |
| Clinical history, including medications   | X               |                |
| Initial assessment of the activities of daily living  | X               |                |
| Initial assessment of behavioral health status, including cognitive functions   | X               |                |
| Initial assessment of psychosocial issues   | X               |                |
| Evaluation of cultural and linguistic needs, preferences or limitations   | X               |                |
| Evaluation of visual and hearing needs, preferences or limitations  | X               |                |
| Evaluation of caregiver resources and involvement   | X               |                |
| Evaluation of available benefits  | X               |                |
| Evaluation of available community resources   | X               |                |
| Assessment of life-planning activities  | X               |                |
| CM plan including prioritized goals, that take into account Member and care givers' goals, preferences and desired level of involvement | X               |                |
| Identification of barriers to meeting goals and complying with the plans  | X               |                |
| Development of schedules for follow-up and communication with Members   | X               |                |
| Development and communication of Member self-management plans   | X               |                |
| Assessment of progress against case management plans and goals, and modification as needed  | X               |                |
| Date CCM terminated   | X               | X              |

## DELEGATION OF DISEASE MANAGEMENT ATTACHMENT

This **Delegation of Disease Management Attachment** (“DM Attachment”) is hereby made part of and incorporated into the Agreement and the Delegation Services Addendum, entered into between **<Insert Name of the Delegator Humana entity> (Delegator)**, and **<Insert Name> (Delegate)** on **<Date>**. This DM Attachment is intended to amend the terms and conditions of the Addendum and to the extent that this DM Attachment conflicts with the terms and conditions of the Agreement or the Addendum, including any prior agreements, addenda, exhibits, or attachments, this DM Attachment controls the relationship between the parties.

### ARTICLE I DELEGATE’S OBLIGATIONS

**Delegate** agrees that it shall:

- 1.1 Acknowledge and agree that **Delegate’s** policies and procedures are subject to **Delegator’s** review and written approval prior to any delegation of Disease Management (DM) functions.
- 1.2 Accept the responsibility and the obligation for performing all DM delegated functions and activities specified in **TABLE 1**, which is attached hereto and incorporated by reference herein, as they relate to services rendered to Members assigned to physicians, employees, Subcontractors and independent contractors.
- 1.3 Acknowledge and agree that clinical assessments of Members are required to be performed by licensed registered nurses (RN) in accordance with nurse practice guidelines and licensure requirements.
- 1.4 Comply with **Delegator’s** policies, procedures, and program requirements and all applicable state and federal laws, rules and regulations and Accreditation Organization requirements pertaining to DM and the delivery of medical and related health care services.
- 1.5 Demonstrate **Delegate’s** DM program plan, previous plan evaluation, and subsequent revisions have been approved by **Delegate’s** internal quality/utilization management (UM) committee.
- 1.6 Not provide incentives to deny, limit, or discontinue Medically Necessary services. Nothing contained in this DM Attachment or the Agreement is intended by **Delegator** to be a financial incentive or payment, which directly or indirectly acts as an inducement for the **Delegate** to limit Medically Necessary services.
- 1.7 Retain all Member-related information and records created for a period of not less than ten (10) years.
- 1.8 Acknowledge that **Delegator** retains all other DM functions not specified as the **Delegate’s** responsibility in this DM Attachment.

### ARTICLE II ACCESS, AUDIT, AND OVERSIGHT

**Delegate** agrees that it shall:

- 2.1 At least annually, or more frequently if deemed necessary by **Delegator**, and then upon not less than ten (10) business days prior notice, or such shorter notice as may be imposed on **Delegator** by a federal or state regulatory agency or Accreditation Organization, allow **Delegator**, its designee, and any state or federal entity or Accreditation Organization to access all DM documentation, processes, policies, systems, and files in order to perform an audit review of the **Delegate’s** policies and procedures, program plan, QI/UM Committee meeting minutes that have been approved by the **Delegate’s** QI/UM Committee, and **Delegate’s** performance/compliance under this DM Attachment. In-person or telephonic/virtual meetings with participation of both **Delegator** and the **Delegate** will be held to discuss results of audits or reports on an as needed basis.

- 2.2 Submit to **Delegator**, with respect to delegated functions, all required reports and analyses, as indicated in **TABLE 2**, which is attached and hereby incorporated by reference, along with identified problems, corrective actions initiated, and outcomes.
  - c. All reports and subsections of reports must be specific to line of business and offering **Delegator's** affiliate, and all reporting formats must be pre-approved by **Delegator**.
  - d. The analysis of data must address identified opportunities for improvement with dates that documented interventions were implemented. The next scheduled report must address follow up activities, outcomes and/or status.
  - e. **Delegate** agrees to provide any and all reports requested by **Delegator** within timeframes identified by **Delegator** to ensure **Delegator** meets all new and revised **Delegator**, CMS, Federal, State and Accreditation Organization reporting requirements.
- 2.3 Acknowledge and agree that **Delegator** maintains the ultimate responsibility for the sufficiency and appropriateness of the DM programs and retains the right to implement a Corrective Action Plan (CAP), suspend or terminate any of this DM Attachment at any time **Delegate** fails to meet or comply with **Delegator's** policies, procedures, and program requirements and all applicable state and federal laws, rules and regulations and Accreditation Organization requirements.
- 2.4 Should the **Delegate** be placed on a CAP, the **Delegate** will have fourteen (14) calendar days to provide a written response describing how they will meet the requirements found to be noncompliant including prospective date of compliance.
- 2.5 **Delegate** will be subject to a capitation payment penalty as indicated in the table below for any outstanding issues noted on a CAP:

| <b>Outstanding Corrective Action Plan</b> | <b>0 to 3 months</b> | <b>4-6 months</b>                      | <b>7-9 months</b>                      | <b>10-12 months or greater</b>         |
|---|----------------------|--|--|--|
| <b>Payment Penalty</b>                    | <b>0%</b>            | <b>1% per month until CAP resolved</b> | <b>2% per month until CAP resolved</b> | <b>3% per month until CAP resolved</b> |

**ARTICLE III  
MEMBER APPEALS AND GRIEVANCES/COMPLAINTS**

- 3.1 **Delegator's** Member expedited and standard complaints/appeals/grievances are not delegated. **Delegator** maintains all Member rights and responsibility functions. **Delegator** will handle all Member appeals/ grievances/complaints for denied services including expedited and standard complaints/appeals/grievances made by a physician/practitioner on behalf of the Member.
- 3.2 **Delegate** will redirect any complaint/grievance and appeal received verbally or in writing to the **Delegator** within one (1) Business Day.
- 3.3 **Delegate** will fax all expedited appeals/grievances/complaints to **Delegator** immediately upon notification/receipt.

**For Expedited and Standard Member Appeals and Grievances/Complaints:**

**Medicare:**  
 Telephone- 1-800-867-6601      Fax- 1-800-949-2961  
**Medicaid:**  
 Telephone- 1-800-764-7591      Fax- 1-855-336-6220

**Commercial:**

Telephone- 1-888-259-6767 Fax- 1-920-339-2112

**FL Medicaid only:**

Telephone- 1-800-477-6931 Fax- 1-800-949-2961

**ARTICLE IV  
TERMINATION**

- 4.1 Notwithstanding anything to the contrary in this DM Attachment, the Addendum, or the Agreement, performance under this DM Attachment may be terminated without cause by either party upon written notice provided to the other party no less than ninety (90) calendar days preceding the termination date or by mutual agreement.
- 4.2 Notwithstanding anything else in this DM Attachment, any breach related to **Delegate's** accreditation and/or licensure, quality assurance issues or alleged breach regarding termination by **Delegator** in the event **Delegator** determines that **Delegate's** continued performance of the delegated functions and/or activities under this DM Attachment may affect adversely the health, safety or welfare of any Member or bring **Delegator** or its provider networks in to disrepute, shall be considered non-curable.

The **Effective Date** of this Disease Management DM Attachment is:                     <Insert Date>                    .

**TABLE 1  
DISEASE MANAGEMENT FUNCTIONS**

| DELEGATED DISEASE MANAGEMENT ACTIVITIES   | DETAIL FUNCTION FOR DELEGATOR   | DETAIL FUNCTION FOR DELEGATE   |
|---|---|--|
| <p><b>Delegate’s Disease Management Programs</b><br/> <b>List the DM Programs:</b><br/>                     Congestive Heart Failure (CHF)<br/>                     Chronic Obstructive Pulmonary Disease (COPD)<br/>                     Coronary Artery Disease (CAD)<br/>                     Diabetes<br/>                     End-Stage Renal Disease (ESRD)</p> |   | <p>Disease Management Programs will be based on adopted Clinical Practice Guidelines.</p>  |
| DM Program  |   | <p><b>Delegate’s</b> DM Program/s will be based on nationally recognized clinical practice guidelines and describe the chronic illness/es of those Members served by the program, the types of services offered including the scope of services, (interventions, communications, self-care training) and a description of the types of measures that are used to assess program performance, including significant outcomes (clinical, satisfaction and costs).</p>  |
| DM Program Participation Criteria   |   | <p><b>Delegate</b> establishes criteria for participation, describes how it monitors the progress of its DM participants, how frequently this occurs.</p>  |
| Identification of Members who qualify for DM programs   | <p><b>Delegator</b> will assist <b>Delegate</b> in providing reporting data as requested by <b>Delegate</b></p> | <p>The <b>Delegate</b> systematically identifies Members who qualify for each of its DM programs <u>at least monthly</u> using multiple referral and data sources including but not limited to claims, encounters, pharmacy, laboratory results, health appraisals, utilization management, case or care management, health management such as wellness or health coaching programs, electronic health records, physician referrals and Member self-referrals.</p>   |
| Program content requirements  |   | <p>Each DM program must address the following:</p> <ol style="list-style-type: none"> <li>1. condition monitoring to include:                             <ol style="list-style-type: none"> <li>a. self-monitoring;</li> <li>b. medical testing;</li> <li>c. regular clinical and laboratory assessment;</li> <li>d. surveillance of pharmacological management;</li> <li>e. lifestyle management; and</li> <li>f. assessing whether a Member understands a condition.</li> </ol> </li> <li>2. adherence to treatment plans and prescribed medication;</li> <li>3. medical and behavioral comorbidities and other health conditions such as cognitive deficits and physical limitations;</li> <li>4. health behaviors;</li> <li>5. psychosocial issues;</li> <li>6. depression screening</li> <li>7. providing information about the Member’s condition to caregivers who have the Member’s consent including:                             <ol style="list-style-type: none"> <li>a. the condition and treatment plan;</li> <li>b. self-management tools;</li> <li>c. DM program and staff resources; and</li> <li>d. community resources;</li> </ol> </li> <li>8. encouraging patients to communicate with their practitioners about their health conditions and treatment; and</li> </ol> |

| DELEGATED DISEASE MANAGEMENT ACTIVITIES   | DETAIL FUNCTION FOR DELEGATOR                                   | DETAIL FUNCTION FOR DELEGATE  |
|---|---|---|
|   |   | 9. additional resources external to the <b>Delegate</b> .   |
| Member communications                     |   | The <b>Delegate</b> will provide the eligible Members the following written information about the program:<br>1. how to use the services;<br>2. how Members become eligible to participate; and<br>3. how to opt in or opt out.   |
| Member interventions                      |   | <b>Delegate</b> will document evidence Member interventions have been performed based on disease stratification and assessment.   |
| Practitioner communications               |   | The <b>Delegate</b> will provide practitioner with the following information about the DM program:<br>1. instructions on how to use DM services; and<br>2. how the <b>Delegate</b> works with practitioner's patients in the program.   |
| Member continuity of care (COC)           |   | The <b>Delegate</b> will integrate information from various systems to facilitate access to Member health information for COC: A health information line; a DM program; a case management program; a UM program; and a wellness program.  |
| Appropriate policies and procedures       |   | <b>Delegate</b> must have documented policies and procedures that meet National Committee for Quality Assurance (NCQA) and Centers for Medicare and Medicaid Services (CMS) requirements, as applicable.  |
| Member experience with disease management | Approve Member satisfaction survey prior to <b>Delegate</b> use | The <b>Delegate</b> annually evaluates the satisfaction with its disease management services by:<br>1. Obtaining and analyzing Member feedback:<br>a. the overall program;<br>b. helpfulness of the program staff;<br>c. usefulness of the information disseminated; and<br>d. Member's experience in adhering to treatment plans<br>2. Analyzing Member feedback and inquiries by conducting a quantitative analysis of data to identify patterns in Member feedback, and conducts a causal analysis if stated goals were not met.   |
| Measure effectiveness of DM Program       |   | The <b>Delegate</b> must track a minimum of one performance measure for each DM program. Each measure:<br>1. addresses a relevant process or outcome;<br>2. produces a quantitative result;<br>3. is population based;<br>4. uses data and methodology that are valid for the process or outcome being measured; and<br>5. has been analyzed in comparison with a benchmark or goal.<br>The <b>Delegate</b> monitors clinical outcomes and measures and tracks performance measures against goals. Results are analyzed; improvement plans are initiated, if warranted. Outcomes in health status for Members are documented. |

**TABLE 3  
DOCUMENTATION REQUIREMENTS**

| <b>Documentation Required</b>   | <b>DM File</b> | <b>DM Log</b>                    |
|---|----------------|----------------------------------|
| Type of DM Program  |                | X                                |
| Line of business  | X              | X                                |
| Member Identification number  | X              | X                                |
| Member name   | X              | X                                |
| Primary Care Physician name   | X              |                                  |
| Names of all involved healthcare professionals including contact information                  | X              |                                  |
| Date enrolled in DM program   | X              | X                                |
| Member diagnoses  | X              | X                                |
| Clinical history including medications  | X              |                                  |
| Disease stratification level and assessment   | X              | X<br>(stratification level only) |
| Development of care plan with ongoing documentation   | X              |                                  |
| Interventions   | X              |                                  |
| Identification of barriers to meeting goals and complying with the plans                      | X              |                                  |
| Development of schedules for follow-up and communication with Members                         | X              |                                  |
| Development and communication of member self-management plans                                 | X              |                                  |
| Assessment of progress against disease management plans and goals, and modification as needed | X              |                                  |
| Date DM program terminated  | X              | X                                |

**TABLE 2  
REQUIRED DISEASE MANAGEMENT REPORTS**

**All reports are to be sent using the secured email procedure and sent to your assigned delegation compliance consultant.**

| MANDATORY REPORTS  | FREQUENCY             | DETAIL   |
|--|-----------------------|--|
| DM Annual Programs   | Annually              |  |
| Previous year DM Programs effectiveness evaluations  | Annually              |  |
| Member DM Program Satisfaction Survey  | Annually              |  |
| Aggregated numbers of all quarterly report data  | Annually              |  |
| Reporting for each delegated DM program of opt-in and opt-out active Member participation rates.   | Quarterly<br>Annually | Report opt-in participation rates:<br>Total eligible population and by condition<br>Number of Members referred to the program and opted in<br>% Members enrolled and actively managed<br>Report opt-out participation rates:<br>Total eligible population and by condition<br>Active participation number<br>% Members opt-out active participation rate |
| Reporting of enrolled Members into <b>Delegate's</b> DM programs. See <b>Table 3</b> for log requirements.   | Quarterly<br>Annually | At a minimum, the annual report is to be submitted to the <b>Delegator</b>   |
| Hospital admissions/readmissions for enrolled DM Members <ul style="list-style-type: none"> <li>• Admissions per each DM program/each total DM program membership</li> <li>• Readmissions per each DM program/each total DM program membership</li> <li>• ER visits per each DM program/each DM program membership</li> </ul>  | Quarterly             |  |
| Member DM Program Satisfaction Survey  | Annually              | Determine performance goals for the Member satisfactory survey and conduct a causal analysis if stated goals were not met.   |
| <p>Note: Reporting requirements may change based upon revised or new state and federal legislation, <b>Delegator</b> and NCQA standards requirements during the term of this Attachment.</p> <p align="center">All reports and subsections of reports must be LOB and <b>Delegator</b> market specific.<br/>The analysis of data and identified opportunities for improvement must include documentation of interventions implemented. Outcomes and/or status should be documented in the next scheduled report. <b>Reporting formats must be pre-approved by Delegator.</b><br/> <b>Monthly</b> – 30 days following the end of the month<br/> <b>Quarterly</b> – 60 days following the end of the quarter<br/> <b>Annually</b> – March 15</p> |                       |  |

**DELEGATION OF QUALITY IMPROVEMENT SERVICES  
FOR BEHAVIORAL HEALTH SERVICES**

**(CONTRACTOR: Delete note - Execute only if function will be performed by an MBHO)**

**ATTACHMENT \_\_**

This **Delegation of Quality Improvement Services Attachment** (“Quality Attachment”) is hereby made part of and incorporated into the Agreement and the Delegation Services Addendum entered into between [ **Humana legal health plan name**] (**Delegator**), and **Name** (**Delegate**). This Quality Attachment is intended to amend the terms and conditions of the Addendum and to the extent that this Quality Attachment conflicts with the terms and conditions of the Agreement or the Addendum, including any prior agreements, addenda, exhibits, or attachments, this Quality Attachment controls the relationship between the parties.

**ARTICLE I  
DELEGATE’S OBLIGATIONS**

**Delegate** agrees that it will:

- 1.1 Accept the obligation to perform all delegated functions and activities for the quality improvement functions and activities described in **Table 1**, which is attached and hereby incorporated by reference, as they relate to services rendered to Members assigned to physicians, employees, sub-delegates and independent contractors.
- 1.2 Comply with **Delegator’s** policies, procedures (Provider Manual), and program requirements, and all applicable state and federal laws rules and regulations and Accreditation Organization requirements pertaining to any quality related activities or services.
- 1.3 Demonstrate **Delegate’s** quality improvement program plan, previous plan evaluation, and subsequent revisions have been approved by **Delegate’s** internal quality improvement committee. Acknowledge and agree that any delegation of quality improvement activities or services is subject to **Delegator’s** review and written approval of **Delegate’s** policies and procedures.
- 1.4 Acknowledge the **Delegator** retains all other quality improvement functions not specified in this agreement as the **Delegate’s** responsibility.
- 1.5 **Delegate** agrees to obtain and or maintain full NCQA/URAC or AAAHC Accreditation status for the term of this contract as required by **Delegator**.

**ARTICLE II  
ACCESS, AUDIT, AND OVERSIGHT**

**Delegate** agrees that it shall:

- 2.1 At least annually, or more frequently if deemed necessary by **Delegator**, and then upon not less than ten (10) business days prior notice, allow access to all quality program documentation, processes, policies, systems, and files to permit **Delegator**, or its designee, to perform an audit review of the **Delegate’s** policies and procedures, program plan, committee meeting minutes that have been approved by the **Delegate’s** Quality Improvement Committee (QI Committee), and **Delegate’s** performance/compliance under this Attachment.
- 2.2 Represent and warrant that it oversees all delegated services in accordance with its policies and procedures and that such policies and procedures are compliant with **Delegator’s** policies and procedures, state and federal laws, rules and regulations, and all Accreditation Organization standards to which **Delegator** is subject, and acknowledges and agree that **Delegate’s** quality improvement policies and procedures are subject to **Delegator’s** review and written approval.

- 2.3 Demonstrate that **Delegate's** quality improvement program plan, previous plan evaluation and subsequent revisions have been approved by **Delegate's** internal QI Committee.
- 2.4 Submit to **Delegator**, with respect to delegated functions, all required reports and analyses, as indicated in **TABLE 2**, which is attached and hereby incorporated by reference, along with identified problems, corrective actions initiated, and outcomes.
- a. All reports and subsections of reports must be specific to line of business and offering **Delegator's** affiliate, and all reporting formats must be pre-approved by **Delegator**.
  - b. **Delegate** agrees to provide any and all reports requested by **Delegator** within timeframes identified by **Delegator** to ensure **Delegator** meets all new and revised CMS, Federal, State and Accreditation Organization reporting requirements.
- 2.5 Should the **Delegate** be placed on a corrective action plan, the **Delegate** will have fourteen (14) calendar days to provide a written response describing how they will meet the requirements found to be noncompliant including prospective date of compliance.
- 2.6 Assure **Delegate's** contracts with practitioners, providers and organization providers specifically require that:
1. Practitioners cooperate with QI activities.
  2. Practitioners maintain the confidentiality of Member information and records.
  3. Practitioners will abide by the **Delegate's** and **Delegator's** policies and procedures.
  4. Practitioners may freely communicate with patients about treatment options available to them, including medication treatment options, regardless of benefit coverage limitations.
  5. Practitioners agree **Delegator** may use the practitioners' performance data.
- 2.7 QI Program Requirements: (including, program description, annual program evaluation, program work plan and formal QI committee)
1. Conducts quality improvement projects (QIP) that can be expected to have a favorable effect on health outcomes and enrollee satisfaction;
  2. Encourages providers to participate in QI initiatives;
  3. Develops and maintains a health information system;
  4. Includes a program review process for formal evaluation that addresses opportunities and activities to improve quality of care and the impact and effectiveness of its QI programs at least annually; and
  5. Has mechanisms to inform Members and providers of the results of the annual evaluation to include the utilization management measures/evaluations.
- 2.8 QI Program Health Information Systems – **Delegate** will:
1. Have the ability to collect, analyze and integrate data necessary to implement their QI program;
  2. Ensure that the information they receive from providers of services is reliable and complete;
  3. Make all collected information available to CMS if requested; and
  4. **Delegate** will collect performance data to assess Member experience and clinical performance.
- 2.9 QI Program Remedial Actions  
For each plan, the **Delegate** must correct all problems which are identified. These problems may be identified through:
1. Internal surveillance;
  2. Complaints;
  3. Plan audits; and

4. Other mechanisms.

- 2.10 Evaluate the continuity and coordination of care furnished to Members. If the **Delegate** uses internally developed as opposed to nationally recognized written protocols for utilization review, the **Delegate** must base those protocols on current standards of medical practice. Mechanisms must be in place to evaluate utilization of services and inform Members and providers of services of the results.
- 2.11 Acknowledge and agree that **Delegator** maintains the ultimate responsibility for the sufficiency and appropriateness of the Quality Improvement Services programs and retains the right to implement a Corrective Action Plan (CAP), suspend or terminate any of this Quality Improvement Services Attachment at any time **Delegate** fails to meet or comply with **Delegator's** policies, procedures, and program requirements and all applicable state and federal laws, rules and regulations and Accreditation Organization requirements.
- 2.12 Should the **Delegate** be placed on a corrective action plan, the **Delegate** will have fourteen (14) calendar days to provide a written response describing how they will meet the requirements found to be noncompliant including prospective date of compliance.
- 2.13 **Delegate** will be subject to a capitation payment withhold as indicated in the table below for any outstanding issues noted on a corrective action plan:

| Outstanding Corrective Action Plan | 0 to 3 months | 4-6 months                       | 7-9 months                      | 10-12 months or greater           |
|------------------------------------|---------------|----------------------------------|---------------------------------|-----------------------------------|
| Payment withholding                | 0%            | .5% per month until CAP resolved | 1% per month until CAP resolved | 1.5% per month until CAP resolved |

**.ARTICLE III  
TERMINATION**

- 4.1 Notwithstanding anything to the contrary in this Quality Improvement Services Attachment, the Addendum, or the Agreement, performance under this Quality Improvement Services Attachment may be terminated without cause by either party upon written notice provided to the other party no less than ninety (90) calendar days preceding the termination date or by mutual agreement.
- 4.2 Notwithstanding anything else in this Quality Improvement Services Attachment, any breach related to **Delegate's** accreditation and/or licensure, quality assurance issues or alleged breach regarding termination by **Delegator** in the event **Delegator** determines that **Delegate's** continued performance of the delegated functions and/or activities under this Quality Improvement Services Attachment may affect adversely the health, safety or welfare of any Member or bring **Delegator** or its provider networks in to disrepute, shall be considered non-curable.

The **Effective Date** of this MBHO Quality Improvement Services Attachment is: <Insert Date>.

TABLE 1

## QUALITY IMPROVEMENT FUNCTIONS

| ACTIVITY   | RESPONSIBILITY OF: |          | DETAIL FUNCTION FOR DELEGATOR   | DETAIL FUNCTION FOR DELEGATE   |
|--|--------------------|----------|---|--|
|  | Delegator          | Delegate |   |  |
| Development and implementation of a Quality Improvement (QI) program encompassing areas beyond Member needs such as clients, providers and other consumers internally and externally   | X                  | X        | Review and approve MBHO's QI program description  | Submit QI Program following approval by MBHO QI Committee  |
| Development and implementation of annual Quality Improvement work plan   | X                  | X        | Review and approve MBHO QI work plan<br>Assure congruence with <b>Delegator</b> QI activities.  | Submit work plan following approval by MBHO QI Committee include preventive health and treatment records   |
| Annual Quality Improvement Program evaluation  | X                  | X        | Review and approve MBHO QI program evaluation   | Submit MBHO QI Evaluation following approval by MBHO QI Committee  |
| Quality of care concern, investigation and resolution  | X                  | X        | <b>Delegator</b> will address incidents and serious QOC concerns through its internal risk management program.<br><b>Delegator</b> will notify Medicaid Member if indicated | Investigate and resolve through QI process. MBHO must report all quality of care concerns to <b>Delegator</b> . Critical incidents must be reported telephonically to <b>Delegator's</b> Risk Management within one business day |
| Quality of care concern, tracking and trending   | X                  | X        | <b>Delegator</b> will review and approve MBHO's trending format or provide recommended format to use  | Include in reports submitted.<br><b>Delegate</b> will be expected to track and trend quality of care concerns to contribute to program improvement activities  |
| Sentinel event investigation, tracking and trending.<br><b>Sentinel Event (also called reportable events/critical incidents)</b> - A term for a 'headliner' event that may cause an unexpected or unanticipated outcome, death or serious physical or psychological injury | X                  | X        | <b>Delegator</b> Risk Manager reports to the state.<br><b>Delegator</b> will provide definition for sentinel events   | Critical incidents must be reported telephonically to <b>Delegator's</b> Risk Management within one business day. MBHO will report tracking and trending of sentinel events in the quarterly QI report                           |
| Verbal Complaints. At least annually analyzes aggregate complaint data in at least the categories of Quality of Care, Access, Attitude/Service, Billing/Financial, and Quality of BH Practitioner Office Site  | X                  |          | <b>Delegator</b> does not delegate complaints   | Request complaint data from <b>Delegator</b>   |
| Member satisfaction survey<br>Annually identifies opportunities for improvement and implement initiatives to improve   | X                  | X        | <b>Delegator</b> shall perform the Member satisfaction survey and share results with the <b>Delegate</b>  | <b>Delegator</b> shall provide the satisfaction survey results and <b>Delegate</b> shall analyze results and report opportunities for improvement back to <b>Delegator</b>   |
| Development, adoption and distribution of behavioral health clinical practice guidelines, at least one of which addresses children and adolescents   | X                  | X        | Approve the MBHO's BH clinical practice guidelines.   | Must be based on nationally recognized sources and incorporate input from community practitioners  |
| Monitoring of adherence to the clinical practice guidelines and measuring the effectiveness of   |                    | X        |   | Measurement no less than annually.   |

| ACTIVITY  | RESPONSIBILITY OF: |          | DETAIL FUNCTION FOR DELEGATOR   | DETAIL FUNCTION FOR DELEGATE  |
|---|--------------------|----------|---|---|
|   | Delegator          | Delegate |   |   |
| at least two aspects of two clinical practice guidelines. One of the clinical practice guidelines measured must address children and adolescents  |                    |          |   |   |
| Continuity and coordination of care with general medical  | X                  | X        | Develop collaborative BH activities, clinical QI study with the health plan. PCP communications to BH clinicians. | Ensure practitioner's communication with <b>Delegator</b> PCP; develop and implement collaborative initiatives. <ol style="list-style-type: none"> <li>1. Exchange of information.</li> <li>2. Appropriate diagnosis, treatment and referral of behavioral healthcare disorders commonly seen in primary care.</li> <li>3. Appropriate use of psychopharmacological medications.</li> <li>4. Management of treatment access and follow-up for Members with coexisting medical and behavioral disorders.</li> <li>5. Primary and secondary preventative behavioral healthcare program implementation.</li> <li>6. Special needs of Members with severe and persistent mental illness.</li> </ol> |
| Appointment availability for emergent-non life threatening, urgent, and routine appointments are offered based on <b>Delegator</b> , federal, state and accreditation requirements (most stringent) |                    | X        |   | Monthly monitoring (reports quarterly to <b>Delegator</b> ). Take actions to ensure standards are met and/or Members are safe with clinical plan. Reports submitted as required by the state or federal regulations. Refer to Service Level Agreement for performance metrics if available. Refer to Table 2  |
| Assessment of Network Adequacy and Opportunities to Improve Access for Members  | X                  | X        | <b>Delegator</b> to provide data from complaints and appeals about network adequacy                               | <b>Delegator</b> to determine if there are issues specific to: Member experience accessing the Network from complaints and appeals about network adequacy, geographic areas or types of providers.<br><b>Delegate</b> shall prioritize opportunities for improvement based upon <b>Delegator's</b> data and annually implement interventions on at least one opportunity and measure the effectiveness of the interventions   |
| Member Telephone access – call blockage rate, abandonment rate and ASA,   |                    | X        |   | Monthly monitoring (reports quarterly to health plan). Take actions as needed to assure performance standards are met. Refer to Table 2.  |
| Quality Improvement Projects: Consumer Organizations  |                    | X        |   | One of the 2 quality improvement projects must address consumer safety for the population served. If the QI project is clinically based, a senior clinical staff person must be involved in judgments with the use of clinical quality measures and clinical aspects of performance   |

**TABLE 2  
REQUIRED QUALITY IMPROVEMENT REPORTING**

Data must be tracked and trended whenever appropriate. Corrective action taken by the **Delegate** must also be reported when appropriate. **All reports are to be sent using the secured email procedure and sent to your assigned delegation compliance consultant.**

| Reporting Category                      | Frequency  | From Delegate to Delegator  |
|---|--|---|
| Quality improvement report              | Quarterly  | Quality improvement report will be submitted and will include: <ul style="list-style-type: none"> <li>• Updates on quality improvement work plan</li> <li>• Corrective actions planned and/or implemented indicated by ongoing monitoring.</li> <li>• Results, analysis, opportunities and interventions updates on clinical quality improvement studies</li> <li>• Changes or modifications to quality improvement program or work plan</li> <li>• New or modified practice guidelines</li> <li>• Summary of quality of care concerns and sentinel events including resolution</li> <li>• Other items as requested by <b>Delegator</b></li> </ul>  |
| Appointment Access                      | Quarterly and Annually                           | Appointment access is offered and based on <b>Delegator</b> , federal and state requirements: <ol style="list-style-type: none"> <li>1. Urgently needed services or emergency- immediate</li> <li>2. Services that are not emergency or urgently needed, but in need of medical attention- within one week</li> <li>3. Routine and preventive care- within 30 days</li> </ol> <b>NCQA Standards:</b> <ol style="list-style-type: none"> <li>1. Care for non-life threatening emergency within 6 hours</li> <li>2. Urgent care within 48 hours</li> <li>3. An appointment for a routine visit within 10 business days</li> </ol> Should apply the most stringent.                          |
| Member Telephone Access                 | Monthly and Report Quarterly to <b>Delegator</b> | Limit average hold time to two (2) minutes<br>Average call abandonment rate not to exceed 5.0%<br>Answer 80% of incoming calls within 30 seconds  |
| MBHO QI Program Description             | Annually   | Submit the MBHO's current year written, annual QI program description   |
| Written evaluation of MBHO QI program   | Annually   | Includes: <ol style="list-style-type: none"> <li>1. A description of completed and ongoing MBHO's QI activities that address quality and safety of clinical care and quality of service</li> <li>2. Trending of measures to assess performance in the quality and safety of clinical care and quality of service</li> <li>3. Analysis and evaluation of the overall effectiveness of the QI program, including progress toward influencing network wide safe clinical practices</li> <li>4. Evaluation of all work plan indicators</li> <li>5. Assessment of adherence to clinical practice guidelines</li> <li>6. Assessment of Member satisfaction survey and complaint data</li> </ol> |
| Written evaluation of MBHO QI work plan | Annually   | Includes: <ol style="list-style-type: none"> <li>1. Quality of clinical care</li> <li>2. Quality of service</li> <li>3. Safety of clinical care</li> <li>4. Program scope</li> <li>5. Yearly objectives</li> <li>6. Yearly planned activities</li> <li>7. Time frame within which each activity is to be achieved and the staff member responsible for each activity</li> <li>8. Monitoring previously identified issues</li> <li>9. Evaluation of the QI program</li> </ol>  |
|   |  |   |

| Reporting Category   | Frequency | From Delegate to Delegator  |
|--|-----------|---|
| Identification of opportunities to improve continuity and coordination of behavioral health care   | Annually  | <ol style="list-style-type: none"> <li>1. Collecting data,</li> <li>2. Conduct quantitative and causal analysis of data to identify improvement opportunities,</li> <li>3. Identify and select two opportunities for improvement</li> </ol>   |
| The collection of data with analysis regarding opportunities for collaboration between medical care and behavioral healthcare  | Annually  | <ol style="list-style-type: none"> <li>1. Exchange of information.</li> <li>2. Appropriate diagnosis, treatment and referral of behavioral healthcare disorders commonly seen in primary care.</li> <li>3. Appropriate use of psychopharmacological medications.</li> <li>4. Management of treatment access and follow-up for Members with coexisting medical and behavioral disorders.</li> <li>5. Primary and secondary preventative behavioral healthcare program implementation.</li> <li>6. Special needs of Members with severe and persistent mental illness.</li> </ol> |
| <p>Note: Reporting requirements may change based upon revised or new state and federal legislation and NCQA standards requirements during the term of this Attachment.</p> |           |   |
| <p><b>Monthly</b> – 30 days following the end of the month<br/> <b>Quarterly</b> – 60 days following the end of the quarter<br/> <b>Annually</b> – March 1</p>             |           |   |

**DELEGATION OF CLAIMS PROCESSING FOR MEDICAL and BEHAVIORAL HEALTH SERVICES  
(remove BH services if not applicable)  
ATTACHMENT**

This **Delegation of Claims Processing Services Attachment** (“Claims Attachment”) is hereby made part of and incorporated into the Agreement and the Delegation Services Addendum, entered into between **<Insert Name of the Humana entity> (Delegator)**, and **<Insert Name> (Delegate)** effective on **<Date>**. This Claims Attachment is intended to amend the terms and conditions of the Addendum and to the extent that this Claims Attachment conflicts with the terms and conditions of the Agreement or the Addendum, including any prior agreements, addenda, exhibits, or attachments, this Claims Attachment controls the relationship between the parties.

**ARTICLE I  
DELEGATE’S OBLIGATIONS**

**Delegate** agrees that it will:

- 1.1 Acknowledge and agree that **Delegate’s** policies and procedures are subject to **Delegator’s** review and written approval prior to any delegation of claims processing functions.
- 1.2 Accept responsibility and the obligation for all claims processing functions delegated hereunder for those services rendered to Members.
- 1.3 Be solely responsible for acquiring, operating, and maintaining any equipment or software necessary in performing its duties hereunder.
- 1.4 Conduct claims adjudication and processing in accordance with **Delegator’s** policies, procedures, and program requirements, Member’s Plan, state and federal laws, rules, and regulations, and the requirements of all regulatory bodies or Accreditation Organizations to which **Delegator** is subject, including but not limited to all privacy and electronic data security laws or regulations, and/or as required by **Delegator**.
- 1.5 Represent and warrant that **Delegate’s** claims processing processes are compliant with the most current American Medical Association (AMA) Current Procedural Terminology (CPT®) code sets, Healthcare Common Procedure Coding System (HCPCS) code sets, International Classification of Diseases, 10th Edition/Revision (ICD-10) code sets (and future ICD revisions when effective), Centers for Medicare & Medicaid Services (CMS) guidelines and national coverage determinations (NCDs), and the CMS National Correct Coding Initiative (NCCI).
- 1.6 Acknowledge and agree that **Delegator** retains the right and final authority to pay any claims for its Members regardless of the delegation of any such functions or activities to **Delegate**.
- 1.7 Acknowledge and agree that any amounts authorized by **Delegate** for payment by **Delegator** may be charged against **Delegate’s** funding.
- 1.8 If required by state and/or federal law, rule or regulation, **Delegate**, at all times during the term of this Addendum, shall obtain, and maintain in good standing a Third Party Administrator (TPA) license/certificate or other state required license/registration/certification. **Delegate** shall provide **Delegator** a copy of the appropriate license/registration/certification number(s) prior to execution of this Addendum and upon renewal thereafter.
- 1.9 Provide a financial guarantee, acceptable to **Delegator** prior to implementation of any delegation of claims processing, including, but not limited to, a letter of credit, to ensure its continued financial solvency and **Delegate’s** ability to adjudicate and process claims hereunder.
- 1.10 **Delegate** shall submit to **Delegator**, financial information, upon request, as proof of their continued financial solvency. Financial information submitted should include the following:
  - a. Recent audited financial statements (balance sheet, statement of operations, statement of cash flows and notes to the financial statements). If the audited financial statements are

over six (6) months old, provide current internal financials with projections (e.g. 6 month-ended financials or quarterly reports).

- b. If **Delegate** has not been audited, **Delegate** is to provide recent internally prepared financial statements (balance sheet, statement of operations and cash flow statement).
- c. **Delegate's** chief financial officer and/or owner will certify/attest to their correctness by adding his/her signature to the financial statements provided to **Delegator**.

- 1.11 **Delegate** agrees to permit any regulatory agency to examine, at any time, information the agency deems relevant to determine the financial solvency of the **Delegate** or to review the **Delegate's** ability to meet its responsibilities in connection with any function delegated to **Delegate** by **Delegator**.
- 1.12 **Delegate** will submit claim/Encounter data in the format defined in the Process Integration Attachment (eConnectivity).
- 1.13 Acknowledge that **Delegator** retains all other claim processing functions not specified as the **Delegate's** responsibility in this Claims Attachment.

## ARTICLE II CLAIMS PERFORMANCE REQUIREMENTS

**Delegate** agrees, and represents and warrants that it will meet, at a minimum, the following claims adjudication and processing performance requirements. **Delegate** must:

- 2.1 Accurately and timely process at least ninety-five percent (95%) of the total of all delegated claims according to **Delegator's** claims processing standards and requirements and in accordance with state and federal laws, rules and regulations and/or the requirements of any regulatory or Accrediting Organization to whom **Delegator** is subject.
- 2.2 Pay any and all statutory interest or other penalties on claims in accordance with applicable state and federal requirements.
- 2.3 Maintain an accuracy rate of at least ninety-nine percent (99%) of total dollars paid, for any given calendar month for all claims processed and adjudicated.
- 2.4 Comply with all state, federal and Accreditation Organization requirements to which **Delegator** is subject with respect to any denial or appeal of claim payment in all communications made to Members. Use **Delegator** prepared Member letter or Explanation of Benefits (EOB) templates for all delegated lines of business as indicated.
- 2.5 Provide claims processing results to **Delegator** on a monthly basis as required by **Delegator's** Delegation Compliance Department using the submission form supplied by **Delegator**.
- 2.6 If processing claims for payment for services rendered to any Medicare Advantage Members, **Delegate** must comply with all rules and requirements for the processing of Medicare Advantage claims established or implemented by the Centers for Medicare and Medicaid Services ("CMS") including, but not limited to, the following:
  - a. the **Delegate** must make correct claim determinations, which include developing the claim for additional information, when necessary, for:
    - 1. Services obtained from a non-contracted provider and reasonable reimbursement when the services were authorized by a contracted provider or the **Delegate**;
    - 2. Ambulance services dispatched through 911;
    - 3. Emergency services;
    - 4. Urgently needed services;

5. Post-stabilization care services;
  6. Renal dialysis services that Medicare Members obtain while temporarily out of the service area; and
  7. Services for which coverage has been denied by the **Delegate** but found to be services the Member was entitled to upon appeal.
- b. Ninety-five percent (95%) of "Clean Claims" (as defined by CMS) from nonparticipating providers must be paid within thirty (30) calendar days of receipt.
  - c. Pay any CMS mandated interest amounts on all Clean Claims which are paid to nonparticipating providers later than thirty (30) calendar days from date of receipt.
  - d. Pay or deny all other claims received by nonparticipating providers within sixty (60) calendar days of receipt.
- 2.7 The **Delegate** is obligated to pay contracted providers under the terms of the contract between the **Delegate** and the Provider.
- 2.8 **Delegate** agrees to include the name of the **Delegate** and the name of the **Delegator** on the remittance document sent to the provider when processing claims and/or making any payment to a health care provider on behalf of the **Delegator**.
- 2.9 **Delegate** agrees that **Delegator** maintains the ultimate responsibility for the accuracy of claims processing and adjudication for Members and retains the right to implement a Corrective Action Plan (CAP), suspend, or terminate any portion of this Claims Attachment in the event there is a breach of this Claims Attachment or noncompliance with state or federal law, Accreditation Organization requirements or **Delegator's** policies, procedures and claims performance requirements.

### ARTICLE III CLAIMS ACCESS, AUDIT AND OVERSIGHT

- 3.1 **Delegate** shall allow **Delegator**, or its designee, to monitor the accuracy, quality, timeliness, and effectiveness of **Delegate's** claims adjudication and processing functions and activities hereunder through periodic reviews and audits. Accordingly, upon request at any time during the term of this Claims Attachment, **Delegate** will provide **Delegator**, or its designee, access to any and all source documentation, and all other documents, processes, procedures, systems and other information related to Member claims processed, paid, denied, or pending hereunder.
- 3.2 Submit to **Delegator**, with respect to delegated functions, all required reports and analyses including but not limited to the contents in **TABLE 1**, which is attached hereto and incorporated by reference herein, along with identified problems, corrective actions initiated, and outcomes.
- a. All reports and subsections of reports must be specific to line of business and offering **Delegator's** affiliate, and all reporting formats must be pre-approved by **Delegator**.
  - b. **Delegate** agrees to provide any and all reports requested by **Delegator** within timeframes identified by **Delegator** to ensure **Delegator** meets all new and revised **Delegator**, CMS, Federal, State and Accreditation Organization reporting requirements.
- 3.3 Should the **Delegate** be placed on a CAP, the **Delegate** will have fourteen (14) calendar days to provide a written response describing how they will meet the requirements found to be noncompliant including prospective date of compliance, which must be remediated within ninety (90) days or less.
- 3.4 **Delegate** will be subject to a capitation payment penalty as indicated in the table below for any outstanding issues noted on a CAP:

| <b>Outstanding Corrective Action Plan</b> | <b>0 to 3 months</b> | <b>4-6 months</b>                      | <b>7-9 months</b>                      | <b>10-12 months or greater</b>         |
|---|----------------------|--|--|--|
| <b>Payment penalty</b>                    | <b>0%</b>            | <b>1% per month until CAP resolved</b> | <b>2% per month until CAP resolved</b> | <b>3% per month until CAP resolved</b> |

**ARTICLE IV  
MEMBER APPEALS AND GRIEVANCES/COMPLAINTS**

- 4.1 **Delegator’s** Member appeals/grievances/complaints are not delegated. **Delegator** maintains all Member rights and responsibility functions. **Delegator** will handle all Member appeals / grievances / complaints regarding claims payment and payment denials including any appeal / grievances / complaints made by a provider on behalf of the Member.
- 4.2 **Delegate** will fax all Member appeals/grievances/complaints to **Delegator** within one (1) business day.

**For Expedited and Standard Member Appeals and Grievances/Complaints:**

**Medicare:**

Telephone- 1-800-867-6601      Fax- 1-800-949-2961

**Medicaid:**

Telephone- 1-800-764-7591      Fax- 1-855-336-6220

**Commercial:**

Telephone- 1-888-259-6767      Fax- 1-920-339-2112

**Florida Medicaid:**

Telephone- 1- 800-477-6931      Fax- 1- 800-949-2961

**ARTICLE V  
PARTICIPATING AND NON-PARTICIPATING PROVIDER DISPUTE/RECONSIDERATION**

**MEDICARE**

- 5.1 **Delegator** will handle all non-participating physician, practitioner, hospital, and other health care professional and/or provider claim payment and payment denial disputes or request for reconsideration.
- 5.2 **Delegate** will fax or instruct the non-participating Provider to fax all disputes/appeals/grievances for claims payments and payment denials within one (1) business day to **Delegator’s** Senior Products Issue Research and Resolution Department.  
Fax Number: 502-508-4565
- 5.2 **Delegate** will handle all participating physician, practitioner, hospital, and other health care professional and/or provider claims payment and payment denial disputes.

- 5.4 **Delegator's** payment dispute/reconsideration determination will be final and processed by **Delegate** as directed.

**COMMERCIAL**

- 5.5 **Delegate** will handle all physician, practitioner, hospital, and other health care professional and/or provider claim payment and payment denial disputes/appeals/grievances for Participating and non-participating Providers except as otherwise required by state or federal law.

**MEDICAID**

- 5.6 **Delegator** will handle all non-participating physician, practitioner, hospital, and other health care professional and/or provider claim payment and payment denial disputes or request for reconsideration.
- 5.2 **Delegate** will fax or instruct the non-participating Provider to fax all disputes/appeals/grievances for claims payments and payment denials within one (1) business day to **Delegator's** Senior Products Issue Research and Resolution Department.  
Fax Number: 502-508-4565
- 5.2 **Delegate** will handle all participating physician, practitioner, hospital, and other health care professional and/or provider claims payment and payment denial disputes.
- 5.4 **Delegator's** payment dispute/reconsideration determination will be final and processed by **Delegate** as directed.

**ARTICLE VI  
TERMINATION**

- 6.1 Notwithstanding anything to the contrary in this Claims Attachment, the Addendum, or the Agreement, performance under this Claims Attachment may be terminated without cause by either party upon written notice provided to the other party no less than ninety (90) calendar days preceding the termination date or by mutual agreement.
- 6.2 Notwithstanding anything else in this Claims Attachment, any breach related to **Delegate's** accreditation and/or licensure, quality assurance issues or alleged breach regarding termination by **Delegator** in the event **Delegator** determines that **Delegate's** continued performance of the delegated functions and/or activities under this Claims Attachment may affect adversely the health, safety or welfare of any Member or bring **Delegator** or its provider networks in to disrepute, shall be considered non-curable.
- 6.3 If delegated for claims payment, the **Delegate** is obligated to pay claims incurred up to the date of termination. The run-off period to pay claims post-termination will be determined by the **Delegator** and shall continue until the last outstanding claim has been paid. The **Delegate** shall continue with the Mandatory Monthly Claims Reporting noted in the Claims Attachment, Table 1, until all applicable claims are paid.

The **Effective Date** of this Claims Attachment is:           <Insert Date>          .

**CLAIMS REPORT TABLE 1**

| <b>MANDATORY REPORTS</b>   | <b>FREQUENCY</b> | <b>DETAIL</b>   |
|--|------------------|---|
| <b>Delegator</b> Monthly Claims Report   | Monthly          | Template will be provided to <b>Delegate</b>  |
| Non-participating Provider Disputes  | Monthly          | Template will be provided to <b>Delegate</b> or <b>Delegator</b> will review <b>Delegate</b> template |
| Medicare Part C Reporting (Requirements can be found in the Medicare Part C Specification Documents)   | Quarterly        | This must be reported 15 days following the end of the quarter.                                       |
| <p><b>Note:</b> Reporting requirements may change based upon revised or new <b>Delegator</b>, state and federal legislation during the term of this Attachment. The Mandatory Reports listed above are in addition to required reports communicated throughout other contract documents.</p> |                  |   |
| <p>All reports and subsections of reports must be line of business (LOB) and <b>Delegator</b> market specific. Reporting templates not provided by <b>Delegator</b> are subject to review and approval.</p>  |                  |   |
| <p><b>Monthly</b> – 15<sup>th</sup> of the following month<br/> <b>Quarterly</b> – April 15, July 15, October 15, January 15</p>   |                  |   |

**FDR COMPLIANCE PROGRAM REQUIREMENTS  
ATTACHMENT \_**

This **FDR Compliance Program Requirements Attachment** (“FDR Attachment”) is hereby made part of and incorporated into the Delegation Services Addendum, entered into by and between **<Insert Name of the Delegator entity> (Delegator)**, and **<Insert Name of Delegate> (Delegate)**. This FDR Attachment is intended to amend the terms and conditions of the Addendum and to the extent that this FDR Attachment conflicts with the terms and conditions of the Addendum, including any prior agreements, addenda, exhibits, or attachments, this FDR Attachment controls the relationship between the parties.

Delegate shall abide by the **FDR Compliance Program Requirements** set forth below, which supplement the requirements under the Addendum in performing any delegated services or functions for Delegator, or Members. These requirements apply to Delegate and its employees that perform or support any delegated services or functions. Delegate shall require materially similar actions on the part of any Downstream Entity Subcontractors which Delegate utilizes in support of the delegated services or functions under this Agreement.

1. Definitions

- A. Downstream Entity: An entity with an indirect contract with Delegator, meaning the contract exists between a First Tier Entity and a Subcontractor or, additionally between that Subcontractor and another Subcontractor down the stream for the performance of Covered Services or any delegated service or function.
- B. First Tier Downstream or Related Entity (FDR): A First Tier Entity, Downstream Entity or Related Entity that is directly or indirectly contracted with the Delegator, as described in the separate defined terms.
- C. First Tier Entity: An entity that has a direct contract with the Delegator or a Delegator -owned entity to provide Covered Services or any delegated service or function that is ultimately the responsibility of the Delegator.
- D. Related Entity: An entity related to Delegator or the Delegate by common ownership or control.

2. FDR Compliance Program Requirements:

- A. Written Policies, Procedures, and Standards of Conduct. Delegator distributes its compliance policy, standards of conduct, general compliance training and fraud, waste, and abuse (“FWA”) training to all First Tier Entities. Delegate is required to comply with these documents and to provide them or materially similar documents and training to their employees and Subcontractors.
- B. Training and Education. Delegate must maintain effective training and educational materials on general compliance and fraud, waste, and abuse consistent with the Center for Medicare and Medicaid Services (CMS) requirements. Education and training completion must be formally tracked and conducted by Delegate within ninety (90) days of initial contract or employment and annually thereafter for all employees.
- C. Exclusion List Screening. Screening against the Office of Inspector General (OIG) and the General Services Administration (GSA) exclusion lists must be conducted by the Delegate prior to hire or contract and at least monthly thereafter. This includes all employees of the Delegate supporting any delegated service or function. Any individual or entity appearing on either list must be promptly removed from supporting any services or functions Delegator has delegated to the Delegate and the Delegator should be notified immediately.

- D. Monitoring and Auditing. Delegate is required to maintain monitoring and auditing work plans to provide oversight of compliance with these policies and related requirements by any Downstream Entities supporting any delegated service or function.
- i. Delegate shall comply and cooperate with any Delegator or CMS-initiated audits related to this Agreement and all related Delegator and CMS policies and regulations, as applicable.
  - ii. Delegator retains the right to audit Delegate at Delegator's discretion for matters related to these policies and requirements.
  - iii. Record Retention. Documentation and records integral to this Agreement and related policies, requirements and activities must be maintained for a minimum of ten (10) years following the termination of the Agreement. This retention requirement includes but is not limited to compliance training record completion; OIG/GSA screening evidence; documentation of any potential or confirmed compliance and/or fraud, waste and abuse issues.
- E. Designated Compliance Resource and High Level Oversight. Delegate must have designated personnel accountable for overseeing compliance responsibilities and to provide high level oversight of compliance obligations.
- F. Investigation, Discipline, and Corrective Actions. Delegate is required to promptly investigate suspected violations of Delegator's policies and requirements and related CMS laws, rules, regulations and instructions, take applicable disciplinary action, and implement any necessary, subsequent corrections to prevent future violations. Additionally, Delegate must widely publicize disciplinary standards and the requirement to report suspected violations. Any violations must be reported to Delegator and Delegate must also cooperate with any Delegator and/or CMS investigation.
- G. Effective Lines of Communication. Delegate is given access to Delegator's compliance officer for feedback and multiple methods for reporting suspected or detected noncompliance. Such reporting is required of all who support Delegator's business and any delegated service or function. Delegate is required to have and publicize one or more reporting options with these features and/or publicize Delegator's reporting options. Delegate must have a widely-publicized policy that prohibits intimidation or retaliation against anyone making a good faith report of suspected violations of related policies and requirements.
- H. Conflicts of Interest. Delegate is required to have a policy on identifying and reporting conflicts of interest. Identified conflicts must be removed or receive approval of the potential conflict.
- I. Requirements of Delegate for Subcontracting Any Delegated Contractual Obligations. The Delegate must:
- i. Notify Delegator when it seeks to subcontract any delegated service or function work and obtain Delegator's approval or rejection of the proposed subcontracted relationship.
  - ii. Maintain written agreements that satisfy applicable state or federal requirements with any Subcontractors or any Downstream Entity supporting delegated functions or services the Delegate is contracted to perform.

- iii. Provide performance and compliance oversight of Subcontractors to assure they are meeting related requirements outlined in any contracts as well as these FDR Compliance Program Requirements.

3. FDR Compliance Contact Information:

A. Delegate shall provide updated and current compliance contact information to Delegator by email to [partnercompliance@humana.com](mailto:partnercompliance@humana.com).

B. Current Compliance Contact Information:

Name: \_\_\_\_\_

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

Phone Number: \_\_\_\_\_

Email Address: \_\_\_\_\_

## PROCESS INTEGRATION ATTACHMENT \_\_\_\_

This Process Integration Attachment (PI Attachment) is hereby made part of and incorporated into the Agreement **Type Agreement** with **Name of Provider (Provider Type)**, which was effective on Effective Date (Agreement). This PI Attachment is intended to amend the terms and conditions of the Agreement and to the extent that this PI Attachment conflicts with the terms and conditions of the Agreement, including any prior Addendums, addenda, exhibits, or attachments, this PI Attachment controls the obligations of the Parties.

In consideration of the mutual promises and covenants herein, the sufficiency of which is acknowledged by the parties, the parties agree as follows:

### ARTICLE I DEFINITIONS

- 1.1 **Claim(s)** means a bill, statement, payment advice, or other request for payment for health services submitted electronically or on UB-04 or HCFA/CMS-1500 forms, or other such successor or replacement forms if submitted as a paper claim.
- 1.2 **Covered Services** means health services provided to Members for which benefits are payable under a Member's health benefits contract or plan.
- 1.3 **Encounter** means data relating to any treatment or service rendered by a provider to a Member, regardless of whether the provider was reimbursed on a capitated or fee-for-service basis or if the service was denied, which is used in determining the level of service provided.
- 1.4 **Health Care Claims** are encounters, delegated encounters and misrouted claims to **Humana**. This definition now aligns with the Health Care Industry's HIPAA Implementation.
- 1.5 **HIPAA** means the Federal privacy regulations developed by the U.S. Department of Health and Human Services at 45 C.F.R. Parts 160, 162 and 164, Security Standards for the Protection of Electronic Health Information and the Standards for Privacy of Individually Identifiable Health Information promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 42 U.S.C. §§1320d-1329d-8; (ED 4/15/2003) as amended, and 45 C.F.R. Part 162, Health Insurance Reform; Modifications to the Health Insurance Portability and Accountability Act (HIPAA) Electronic Transaction (ED 01/16/2009) as amended, and the Health Information Technology for Economic and Clinical Health Act (HITECH), enacted as part of the American Recovery and Reinvestment Act of 2009 (ED 2/18/2009) as amended.
- 1.6 **Member** means any person who is eligible to receive Covered Services and who is enrolled in a health benefit plan which utilizes one of the **Delegator** networks.
- 1.7 **Trading Partner(s)** means a Delegate or other party with whom **Delegator** has a contracted business relationship that involves the exchange of data by means of electronic transactions.

### ARTICLE II Delegate Claims Processing Obligations

- 2.1 Produce and submit Health Care Claims in accordance with state and federal laws, rules, and regulations, and the requirements of all regulatory bodies or Accreditation Organizations to which **Delegator** is subject, including but not limited to all privacy and electronic data security laws or regulations, and/or as required by **Delegator**.

- 2.2 Provide **Delegator** with accurate and complete Health Care Claims in an electronic, HIPAA-compliant format that mirrors the provision of Covered Services provided to Members (“Encounter”).
- 2.3 **Delegate** shall submit Health Care Claims at a minimum once per calendar week via HIPAA-compliant Ansi X12 837 Health Care Claim format. At a minimum Health Care Claims shall include accurate Member identification and demographic information; **Delegate** and/or **Delegate** physician tax identification number; billing provider NPI number; “pay to” provider NPI number; rendering provider NPI number; date of service; all applicable CPT, ICD, revenue and HIPAA codes; amount provider billed, total cost (amount **Delegate** approved), **Delegate’s** share and Member’s share (any patient out-of-pocket amounts arising from a deductible, Coinsurance or co-pay requirement for that plan coverage) amounts for each line of the Encounter, and any notices of an audit or review performed by the delegated entity of a patient medical record.
- 2.4 The **Delegate** shall refer to the **Delegator** Companion Guide for Delegated Health Care Claims for the specific mapping of this data. **Delegate** agrees to work with **Delegator** to provide any other data required by **Delegator** for proper processing of Health Care Claims.
- 2.5 **Delegate** shall use the most current procedural technology (CPT) codes, ICD diagnosis, and revenue codes. **Delegate’s** system shall be capable of maintaining and transmitting the maximum number of diagnosis codes that can be transmitted in the 837 format (25 plus admitting dx = 26 for institutional claims and 12 for professional claims) per Health Care Claim. **Delegate** shall ensure that all CPT, ICD, and revenue codes utilized will be compliant with Medicare/CMS coding guidelines.
- 2.6 **Delegate** shall:
- a. submit Health Care Claims directly through either Availity or ZirMed.com (“Preferred Clearinghouse”); or
  - b. submit Health Care Claims through a clearinghouse with confirmed connectivity to one of **Delegator’s** direct connected Trading Partners, Availity or ZirMed; and
  - c. provide **Delegator** with a summary list of Health Care Claims (“Shadow File”) that reflect all paid and adjudicated claims delegated Members or as requested by **Delegator** EDI. The Shadow File layout shall identify the minimum data set requirement needed to conduct the reconciliation process for Health Care Claims. Shadow files shall be made available as frequent as on a quarterly basis or a minimum of two (2) times per year prior to CMS sweeps deadline. Shadow files and/or other reporting and data requests may be posted or made available on the Provider Portal at **Delegator’s** designated location.
- 2.7 **Delegate** shall correct and resubmit any and all Health Care Claims that are rejected by a clearinghouse for edit issues within seven (7) calendar days of notification. Additionally, **Delegate** shall correct data deemed inconsistent, lacking specificity, or otherwise inaccurately identifying the Member or services provided as determined by **Delegator**.
- 2.8 **Delegate** acknowledges and agrees that Health Care Claims shall be submitted to **Delegator** electronically within a calendar week of the date the claim was processed. **Delegate** shall submit Health Care Claims that pass Level 7 HIPAA compliance requirements:
- 2.9 **Delegate** acknowledges and agrees that Health Care Claims shall be submitted to **Delegator** which includes Member Out-of-Pocket (“MOOP”) cost by utilizing the HIPAA compliant technology specified by the **Delegator**. **Delegator** shall provide file specifications upon execution of this agreement.

- 2.10 Any failure by Delegate to comply with these provisions may result in the immediate suspension or revocation of all or any portion of any delegated Claims activities functions at Delegator's discretion.

## INFORMATION TECHNOLOGY SECURITY ATTACHMENT

This Information Security Agreement (hereinafter, the "ISA") is issued pursuant to and attached to the [Enter the title of the governing agreement] by and between [Enter Vendor Name] (hereinafter "Vendor") and Humana Inc. (hereinafter "Customer") effective on or about [Enter Effective Date of Governing Agreement] (hereinafter the "Agreement"). Any term not otherwise defined herein shall have the meaning ascribed to it in the Agreement. This ISA is effective on [Choose One - «Effective date» OR date of last signature] (the "Effective Date"). In the event of an express conflict between this ISA and the Agreement, the terms of this ISA shall control with respect to the specific subject matter hereof.

WHEREAS, the parties recognize that information security practices play an important role in their relationship;  
and

WHEREAS, the parties recognize that unauthorized disclosure of information can be detrimental to both parties;  
and

WHEREAS, the parties recognize that unauthorized disclosure of information may result in significant penalties;  
and

WHEREAS, the parties wish to memorialize those information security practices to which they shall adhere;

NOW THEREFORE, Customer and Vendor hereby agree as follows:

### **1. Definitions. For purposes of this ISA, the following definitions shall apply:**

- a) "Business Associate" means Vendor acting as a Business Associate as such term is defined in 45 C. F. R. 160.103.
- b) "Cardholder Data" means the full magnetic stripe data or the Primary Account Number ("PAN") and any or all of the following: cardholder name, approval code, or expiration date.
- c) "Computer Security Incident" or "Incident" as defined in the National Institute of Standards and Technology (NIST) special publication (SP) 800-61 rev.2 means a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
- d) Unless otherwise defined in the Agreement, "Customer Confidential Information" means:
  - i) trade secrets, all past, present and future business activities and all information related to the business of Customer, its parent company and its subsidiaries and affiliated companies and its or their clients, members and/or enrollees, that may be obtained from any source, whether written or oral, as well as all information on Customer's mainframe, networks, local-area networks ("LAN") and workstations and all software, middleware, firmware, groupware and licensed internal code whether owned or licensed currently or in the future by Customer and accessed by Vendor or any of Vendor's employees, contingent workers and subcontractors (such Vendor employees, contingent workers and subcontractors collectively referenced hereinafter as "Representatives") by any direct or remote access method and also including, but not limited to, any information relating to the pricing, software or technical information, hardware, methods, processes, financial data, compilations, lists, apparatus, statistics, program, research, development or related information of Customer, its subsidiaries or affiliated companies or its clients, patients, members and/or enrollees concerning past, present or future business activities of said entities, and/or the results of any analysis of any of the foregoing and outcome of any provision of services by Vendor and Representatives under this Agreement, provided that disclosure of the foregoing in response, and only to such extent and for such purpose, to a valid order by a court of competent jurisdiction or as otherwise required by law shall not be considered a breach of Vendor's duty under this ISA to hold Customer Confidential Information in strict confidence.
  - ii) Customer Confidential Information does not include information that:
    - (1) has been previously published or is now or becomes public knowledge through no fault or negligence of Vendor or Representatives; or

- (2) can be established by documentary evidence to have been made available to Vendor or Representatives, without restriction on disclosure, by a third-party not under obligation of confidentiality with respect to the disclosed information; or
  - (3) can be established by documentary evidence to have been independently developed by Vendor or Representatives.
- e) “Customer Information Systems” means information systems resources supplied and operated by or on behalf of Customer, including but not limited to, contracted IaaS, PaaS, SaaS cloud services, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, proprietary applications, printers, and internet connectivity that are owned, controlled, or administered by Customer.
- f) “Information Security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- g) “Multi-Function Device” or “MFD” means an office machine which incorporates the functionality of multiple devices in one. A typical MFD may provide a combination of some or all of the following services:
  - i) Printing
  - ii) Scanning
  - iii) Photocopying
  - iv) Faxing
  - v) Emailing
- h) “Payment Card Industry Data Security Standards” or “PCI DSS” means the information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards as defined by the Payment Card Industry Security Standards Council. The standard was created to increase controls around Cardholder Data to reduce credit card fraud via its exposure. A current version of the standard may be obtained from <https://www.pcisecuritystandards.org/>.
- i) “Personal Computer” or “PC” means any laptop, notebook, desktop, netbook, or any other personal computing apparatus or device which is used to access, process, or display information. This definition does not include computing devices operating as servers in a hardened, controlled access, secured data center.
- j) “Protected Health Information” or “PHI” shall have the same meaning as the term “Protected Health Information” as defined by 45 C. F. R. 160.103, limited to the information created or received by Vendor, acting as a Business Associate of Customer, from or on behalf of Customer.
- k) “Security Breach” means the unauthorized acquisition, access, use, or disclosure of information which compromises the security or privacy of such information, except where an unauthorized person, to whom such information is disclosed, would not reasonably have been able to retain such information. Security Breach does not include:
  - i) Any unintentional acquisition, access, or use of Customer Confidential Information by an employee or individual acting under the authority of Vendor if:
    - (1) such acquisition, access or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with Vendor; and
    - (2) such information is not further acquired, accessed, used, or disclosed by any person; or

- (3) Any inadvertent disclosure from an individual who is otherwise authorized to access Customer Confidential Information at a facility operated by Vendor to another similarly situated individual at the same facility; and
  - (4) Any such information received as a result of such disclosure is not further acquired, accessed, used or disclosed without authorization by any person.
- l) “Services” shall have the same meaning as in the Agreement.
  - m) “Vendor Representative” means an employee, contractor, or agent of Vendor, or of its subcontractors and contingent workers, who provide Services to Customer.
  - n) “Vendor Processing Resources” means information processing resources supplied or operated by Vendor, including without limitation, contracted IaaS, PaaS, SaaS cloud services, network infrastructure, computer systems, workstations, laptops, hardware, software, databases, storage media, printers, proprietary applications, Internet connectivity, printers and hard copies which are used, either directly or indirectly, in support of Vendor processing.

## 2. Provisions applicable for ALL Vendors

### a) General Requirements

- i) Vendor shall not collect or generate metadata related to Customer or its members for any purpose other than to provide the Services for which the Vendor has been engaged by Customer.
- ii) Telemetry data collected to monitor operational health of a system must not contain protected information. If telemetry captures protected information as part of its monitoring function, the telemetry data must be protected and handled commensurate with the information’s security requirements. Any telemetry data found to contain protected information not being protected appropriately will be interpreted as an exposure until proven otherwise.
- iii) Unless previously authorized by Customer in writing, all work performed by Vendor related to the Agreement shall be performed from the secured Vendor Facilities located at the Vendor location(s) designated in the Agreement and/or relevant statement(s) of work.
- iv) Vendor shall only have access to Customer Information Systems authorized by Customer and shall use such access solely for providing Services to Customer. Vendor shall not attempt to access any applications, systems, or data which Customer has not authorized Vendor to access, nor shall Vendor use access credentials to create automated processes except as authorized in a fully executed statement(s) of work. If authorized, Vendor shall access and use such applications, data, and systems only as minimally necessary to provide Services to Customer and solely for such purposes. Vendor's attempt to access any applications, data, or systems in violation of the terms of Section 2 shall constitute a material breach of the Agreement.
- v) Although the security and confidentiality requirements specified herein are minimum standards intended to facilitate the protection of Customer Confidential Information, it remains Vendor’s responsibility to take appropriate additional measures and precautions necessary to ensure the confidentiality, availability, and integrity of Customer Confidential Information.

### b) Information Security Policies

- i) Vendor shall have a security control framework based upon an accepted standard governing the information security within Vendor’s industry (e.g., NIST, HITRUST, ISO, etc.). Such framework shall utilize a standard set of controls, and shall be meant to include, but not be limited to, commercially available and widespread use of precautionary measures.
- ii) Vendor shall develop and maintain a comprehensive Information Security Policy (“Policy”).

- iii) Vendor shall review the Policy not less than annually and whenever there is a material change in practices or regulatory requirements.
- iv) Vendor shall have a designated employee or group of employees who shall maintain said Policy.
- v) Vendor shall monitor its Policy to ensure that the program described therein is operating in a manner reasonably calculated to prevent unauthorized access.

**c) Physical Security**

- i) Vendor shall maintain appropriate physical security controls, including facility and environmental controls, to prevent unauthorized physical access to Vendor Processing Resources and areas in which Customer Confidential Information is stored or processed. Where practicable, this obligation shall include controls to physically protect hardware (e.g., lockdown devices).
- ii) Vendor shall adopt and implement a written facility security plan which documents such controls and the policies and procedures through which such controls will be maintained.
- iii) Vendor shall maintain appropriate records of maintenance performed on Vendor Processing Resources and on the physical control mechanisms used to secure Vendor Processing Resources.
- iv) Vendor shall notify Customer before moving storage or processing of Customer Confidential Information, or changing the location of a Vendor facility where Services are being provided to any location not previously authorized by Customer. This notification includes movement of contracted cloud services from one cloud service provider to another or to a different geographic data center from the same cloud service provider. Customer reserves the right to inspect such facilities within 180 days of such notification.
- v) Vendor shall restrict entry to Vendor's area(s) where Customer Confidential Information is stored, accessed, or processed solely to Vendor's Representatives with a need to access such area(s) and information and escorted guests.
- vi) Vendor shall implement reasonable best practices for infrastructure systems including, but not limited to, fire extinguishing, cooling, and emergency systems designed to reasonably ensure employee safety.
- vii) Vendor shall provide physical entry controls for all areas where Customer Confidential Information is stored, accessed, or processed that are commensurate with the sensitivity of the Customer Confidential Information; each of Vendor's Representatives accessing these areas must employ one or more unique, individually identifiable entry controls (such as card keys) that provide an audit trail of each entry. All visitors who enter these areas must be logged and escorted, at all times, by one of Vendor's Representatives who are authorized to access such area.
- viii) Vendor shall regularly monitor areas where Customer Confidential Information is handled, stored, and/or processed through the use of appropriate measures such as cameras, guards, and entry logs.
- ix) In situations where a statement of work allows work to be conducted outside of an authorized facility, Vendors shall implement and maintain a set of policies and procedures which provide guidance and instruction on protecting information outside the office.

**d) Risk Management**

- i) Vendor shall develop and use a defined risk assessment methodology.
- ii) Vendor shall conduct risk assessments and reviews upon significant change and in no case less than once per year.
- iii) Vendor will document results of all risk assessments, develop action plans for the mitigation of findings, and track the progress of such action plans.

**e) Configuration and Change Management**

- i) Vendor shall define and control formal, documented configuration and change management policies. Said policies shall address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Vendor shall review said policies and update as needed, but in no case shall such reviews occur less than annually.
- ii) Vendor shall ensure that all changes to systems are documented and follow recognized change control procedures.
- iii) Vendor shall ensure that segregation of duties exists such that the individual or system performing changes is not the same individual or system which approves such changes.

**f) Third-Party Management**

- i) Vendor shall provide to Customer, upon request, information on its third-party security audit processes, procedures and controls, including a summary report on any material findings and remediation efforts relevant to services authorized under the Agreement.
- ii) Unless specifically authorized and agreed to by the parties in a statement of work under the Agreement, Vendor shall not provide or allow access to Customer Confidential Information by any third-party.
- iii) Vendor shall conduct risk assessments and reviews upon all third-parties with access to Customer Confidential Information no less than once per year. A summary of such assessment methodology, along with a summary of results, shall be provided to Customer upon written request.
- iv) Vendor shall be responsible for ensuring all contracted downstream partners and cloud service providers used in the delivery of services authorized under the Agreement meet or exceed the security obligations contained in this ISA.
- v) Vendor shall report to Customer within thirty (30) days of execution of this ISA, and upon any change, the names and locations of all downstream partners with access to Customer Confidential Information, and the nature of the services provided by those partners, that necessitates access to Customer Confidential Information. Vendor shall further report to Customer a consolidated list of the names and all locations of all downstream partners with access to Customer Confidential Information, and the nature of the services provided by those partners that necessitates access to Customer Confidential Information annually.

**g) Mobile Device Security**

- i) Vendor shall ensure that appropriate measures for securing portable devices are explained and followed by all employees, this includes, but is not limited to, any time the device is not in a secured office location (e.g., in automobiles, on aircraft, at home, etc.).
- ii) Vendor shall create and maintain policies and standards which provide guidance on transporting and securing devices which may contain Customer Confidential Information when outside the office.
- iii) Vendor shall ensure that all Vendor owned and Vendor Representative owned mobile devices used to store, process, or transmit Customer Confidential Information are encrypted.

**h) Encryption Requirements**

- i) Vendor shall utilize dedicated encryption keys. All encryption keys used to protect Customer Confidential Information shall be uniquely associated to Customer. The use of said encryption keys to encrypt non-Customer data is forbidden.
- ii) All keys will be protected against modification; secret and private keys need to be protected against unauthorized disclosure.

- iii) FIPS-approved or NIST-recommended cryptographic algorithms commensurate with key size shall be used whenever cryptographic services are applied.
- iv) Vendor shall implement full disk encryption on any built-in or removable storage media in any Vendor controlled portable device which may access, store, process, transmit, or create Customer Confidential Information. All such encryption shall minimally meet the Advanced Encryption Standard with a 256-bit cypher key (“AES-256”) as outlined in the Federal Information Processing Standards publication 197 (“FIPS 197”).
- v) Vendor shall ensure that all passwords are transmitted securely and encrypted when in storage. In the event that a hashing algorithm is used, Vendor must use a randomly-generated salt.
- vi) Plaintext Encryption and/or Decryption keys must be adequately secured under split knowledge or multi-factor authentication (“MFA”) mechanisms. Only those trusted associates who have a “need to know” should be given access to the key or security environment storing keys. Storage of these keys must be separate and distinct from the encrypted data.
- vii) When a Data Encryption Key (“DEK”) must be stored encrypted in a boot page of a data store, the DEK encryptor (Key Encryption Key (“KEK”)) must be separate and distinct from the encrypted data store and DEK.
- viii) When a cryptographic key is compromised, all use of the key to apply cryptographic protection to information (e.g., compute a digital signature or encrypt information) shall cease, and the compromised key shall be revoked. However, the continued use of the key under controlled circumstances to remove or verify the protections (e.g., decrypt or verify a digital signature) may be warranted. All compromised keys must be retired and replaced in a timely fashion.
- ix) Vendor encryption key management systems shall be designed so that the compromise of a single key compromises as little data as possible and avoids having a catastrophic weakness.
- x) Vendor shall have a compromise recovery plan for restoring cryptographic security services in the event of a key compromise.
- xi) Encryption keys will not persist unencrypted in any environment beyond the minimum time required for use. To the maximum extent operationally possible, plaintext symmetric and private keys are restricted to physically protected containers. This includes key generators, key-transport devices, key loaders, cryptographic modules, and key-storage devices.
- xii) Encryption key metadata is used to identify attributes, parameters, or the intended use of a key, and as such contains the key’s control information. This information requires elevated protection commensurate with Key Management System (“KMS”) access.
- xiii) Vendors will use an accountability system that keeps track of each access to symmetric and private keys in plaintext form.
- xiv) In the event that tapes are used for system backup, such tapes shall be encrypted and appropriately inventoried and logged as to location and planned destruction date.

**i) Remote Computing Requirements**

- i) All permitted and authorized remote sessions that may entail access to Customer Confidential Information shall only be performed via a secure Virtual Private Network (“VPN”).

**j) Malware Protection**

- i) Vendor shall install, enable and keep current reputable, commercially available anti-malware software on all Vendor servers and Personal Computers used in accessing, storing, processing, transmitting, or creating Customer Confidential Information.

**k) Password, Access and Identity Management**

- i) Vendor shall require that all Vendor Representatives with access to Customer Confidential Information use a unique username and password (collectively “Login Credentials”). Each password shall have an effective use period of no more than ninety (90) days. Said password shall be a minimum of eight (8) characters in length and include at least three (3) of the following: alpha, numeric, special character, and case sensitivity. Additionally, said password shall not contain any portion of username, and shall not be reused for a minimum of three hundred sixty-five (365) days.
- ii) Vendor shall ensure that Login Credentials are terminated within twenty four (24) hours following the removal of Vendor Representatives from provision of the Services for any reason.
- iii) Vendor shall use unique logins on all network equipment whenever commercially possible.
- iv) Vendor shall not allow the sharing of passwords.
- v) Vendor shall not allow the use of vendor supplied default credentials.
- vi) Not less than monthly, Vendor shall review access log files for indications of misuse of credentials, including but not limited to, sharing of credentials, sharing of passwords, etc.
- vii) Not less than monthly, Vendor shall review access log files for suspicious login activity. Any such identified activity shall be promptly investigated and appropriately mitigated.

**l) Logical/System Access Control and Monitoring**

- i) Vendor shall implement a formal user registration and deregistration procedure for granting and revoking access to Vendor Processing Resources. Upon termination of any of Vendor Representatives, Vendor shall ensure that such Vendor Representative’s access to Customer Confidential Information is revoked and notification to Customer is made no later than one business day following termination. In the event of an involuntary termination, Vendor shall ensure all access is revoked immediately.
- ii) Vendor shall maintain appropriate access control mechanisms to prevent all access to Customer Information Systems and/or Vendor Processing Resources, except by (a) specified users expressly authorized by Customer and (b) Vendor Representatives who have a “need to access” to perform a particular function in support of Vendor Processing.
- iii) Vendor shall maintain appropriate mechanisms and processes for detecting, recording, analyzing, and resolving unauthorized attempts to access Customer Information Systems or Vendor Processing Resources.
- iv) Vendor shall review access logs not less than quarterly to ensure that access permissions are appropriate and necessary.
- v) Vendor’s operating system security mechanisms must be configured to support appropriate security procedures, and should at a minimum:
  - (1) Identify and verify the identity of each authorized user; and
  - (2) Record successful and failed system accesses.
- vi) Vendor shall ensure that segregation of duties exists such that the individual or system granting access is not the same individual or system which approves such access.

**m) Cloud Computing**

- i) Vendor shall ensure that all Customer Confidential Information stored in any cloud based solution be encrypted per all aforementioned encryption requirements.

- ii) Customer Confidential Information shall be stored in US-based data centers to the greatest extent possible. If overseas data storage is required, only Customer approved geolocations shall be utilized.
- iii) Customer Confidential Information shall be protected by a unique Data Encryption Key (“DEK”) that must not be stored in plaintext. Master Key Encryption Keys (“KEK”), preferably those provided by Customer, will be used to decrypt subordinate DEK’s. All KEK’s regardless of source must be stored in a Federal Information Processing Standards (“FIPS”) 140 certified KMS Hardware Security Module (“HSM”) under split knowledge access controls. Vendor will retain exclusive control of keys and not provide subsequent access to any other entity. Vendors shall ensure a unique KEK is used for DEK’s specific to Customer Confidential Information. Any use of a Customer specific KEK or subordinate DEK for any purposes other than Customer Confidential Information is strictly forbidden.

**n) Vulnerability Management and Patching**

- i) Vendor shall adhere to applicable standards governing the patch management criticality rankings and patching time frame requirements for all systems and applications including, but not limited to, switches, routers, appliances, servers, workstation PC’s, commercial software, and open source software.
- ii) Vendor shall conduct comprehensive scans for known vulnerabilities on all externally facing systems no less than one time per month.
- iii) Vendor shall conduct comprehensive scans for known vulnerabilities on the entire network no less than once per quarter.
- iv) All critical and high vulnerabilities must be remediated within fifteen (15) days of release unless application requirements preclude such patching. Should such preclusion exist, mitigating controls offering the same level of protection must be implemented within the aforementioned time frame.
- v) Vendor shall ensure that all urgent, critical, and high patches are implemented in a timely manner. Urgent and critical patches must be implemented within thirty (30) days of release unless application requirements preclude such patching. Should such preclusion exist, mitigating controls offering the same level of protection must be implemented within the aforementioned time frame.

**o) Secure Disposal**

- i) All media containing Customer Confidential Information shall be disposed of via appropriate physical destruction (e.g., shredding, drilling, crushing, incinerating, etc.). Disposal methodology shall be driven by category of information and NIST guidance on appropriate minimum destruction techniques and procedures. Media shall include any storage capability in owned or leased equipment to include Multi-Function Devices such as leased copy/printer/fax machines.

**p) Vendor Representative Training and Related Matters**

- i) Vendor shall perform criminal background checks on any Vendor Representative with potential access to Customer Confidential Information. Such background checks must be performed prior to allowing such individual to access Customer Confidential Information; and Vendor shall not allow any individual who does not have a satisfactory background check to access Customer Confidential Information.
- ii) Vendor shall require credit checks on all individuals whose duties require them to access credit card or other financial information except to the extent limited or prohibited by applicable laws.
- iii) For any Vendor Representatives that have access to Customer Confidential Information outside the United States, such background checks shall include a nationwide criminal background check to the extent permitted by applicable laws.
- iv) Vendor shall train new Vendor Representatives – including contingent workers – on the acceptable use and handling of Customer Confidential Information.

- v) Vendor shall provide periodic and mandatory Information Security training and awareness to its Vendor Representatives. Such training shall occur not less than annually.

**q) Audit**

- i) Not more than once per calendar year, Customer reserves the right, upon reasonable notice and at Customer's expense, to review said Vendor risk program. This right includes the use of Customer personnel or may be delegated to a third-party.
- ii) In the event of a Computer Security Incident or Security Breach, the calendar limitation listed above is not applicable.
- iii) Customer reserves the right to audit compliance with the subject matter covered within this ISA on an annual basis, onsite at Vendor location. This right includes the use of Customer personnel or may be delegated to a third-party.

**r) Network Controls**

- i) Vendor shall implement appropriate controls to ensure that only authorized devices are provisioned network access when physically connected to the network.
- ii) As necessary, Vendor shall provision logically or physically segregated network to allow guest access for visitors to their facilities. In no case shall Vendor allow guests, or other non-Vendor managed and controlled personnel, access to production networks.
- iii) Vendor shall implement technical controls to filter inappropriate and unnecessary web content including, but not limited to, pornography, gambling, violence, webmail, social media, etc.
- iv) All Vendor controlled wireless connections shall be secured utilizing Wi-Fi Protected Access 2 ("WPA2") or better security protocol.
- v) Vendor shall ensure that interconnections within Vendor, with other companies, and with the Internet ("Access Points"), whether wired or wireless, into the Vendor network are protected by using firewalls, secure tunnels, and/or access lists on routers.
- vi) Vendor shall ensure that a network management system is used to monitor its local network and servers. Thresholds and alarms shall be established to notify Vendor of potential problems or outages.
- vii) Vendor shall implement either host-based or network-based Intrusion Detection Solution ("IDS") or Intrusion Protection Solution ("IPS") on any Vendor controlled network used to process, store, transmit, or access Customer Confidential Information. Appropriate response and recovery plans to monitor potential unauthorized access to said network and systems shall be implemented.
- viii) Vendor shall implement a Data Loss Prevention system ("DLP") to prevent the accidental or intentional distribution of Customer Confidential Information.
- ix) Vendor shall secure all unused network ports.

**s) Transmission Protection**

- i) Vendor shall encrypt all data, records, and files containing Customer Confidential Information, including email, that shall be transmitted wirelessly or travel across public networks.
- ii) Vendor shall require all transmissions of PHI to be secure and encrypted, including but not limited to: email, webmail, mobile device email, FTP, chat and instant messaging, web services, etc.

**t) Incident and Breach Response**

- i) Vendor shall report each Computer Security Incident or Security Breach to Customer in an appropriate and timely manner.
- ii) Vendor shall establish formal Incident response policies and procedures.
- iii) Vendor shall establish formal documented management responsibilities and procedures to ensure a timely, effective, and orderly response to Computer Security Incidents or Security Breaches.
- iv) Vendor shall identify appropriate resources to monitor the internal environment for security events, to evaluate security events, and to respond to Incidents in a timely manner.
- v) In the event of a Computer Security Incident or Security Breach, Vendor shall collect, retain, and present evidence in support of potential legal action in accordance with the rules of evidence in the relevant jurisdiction.
- vi) Vendor shall, if requested, provide applicable information, including but not limited to, forensic copies, network and activity logs, and reasonable access to Vendor Representatives to assist Customer in investigating the Incident.

**u) Security Contact**

- i) Vendor shall assign an individual to act as the primary security liaison (the “Security Custodian”) between Vendor and Customer. This person shall be a trusted source at Vendor for the distribution of passwords and other confidential security matters.

|                          |  |
|--------------------------|--|
| Security Custodian Name: |  |
| Email:                   |  |
| Phone Number:            |  |
| Address:                 |  |
|                          |  |
|                          |  |

- ii) In the event that the above listed person is no longer acting in the role of Security Custodian, Vendor shall notify Customer of said change by sending the above information for the new Security Custodian to [HumanaVendorSecurity@humana.com](mailto:HumanaVendorSecurity@humana.com).

**3. Provisions applicable to all Business Associate Vendors – In addition to Section 2 above, the provisions in this section are applicable to all Vendors who access, store, process, transmit, or create on behalf of Customer or are otherwise exposed to PHI.**

**a) Physical Security**

- i) Vendor shall notify Customer before moving storage or processing of PHI, or changing the location of a Vendor facility where services which involve PHI are being provided to any location not previously authorized by Customer in applicable statement(s) of work. Without regard to frequency language in audit section of this ISA, Customer reserves the right to inspect such facilities within 180 days of such notification.
- ii) Vendor shall only permit access to PHI from work locations specifically outlined in the associated statement of work. If the statement of work does not specify the work location, unless otherwise permitted in a fully executed statement of work, such access to PHI will only occur within secured Vendor controlled facilities.
- iii) Vendor shall restrict entry to area(s) where PHI is accessed, stored, or processed solely to Vendor Representatives authorized for such access.

**b) Offshore Access**

- i) Unless specifically authorized and agreed to by the parties in a statement of work under the Agreement, Vendor shall not access, store, process, transmit, or create PHI at locations outside the fifty (50) United States of America. This prohibition applies not only to Vendor's data center locations primarily involved with providing the services contracted, but equally to any and all data centers used for resilience or redundancy, backups, log storage, and any downstream partners that may access, store, process, transmit, or create PHI.
- ii) Unless specifically authorized and agreed to by the parties in a statement of work under the Agreement, Vendor shall not permit viewing access to PHI by Vendor Representative or any other person outside the 50 United States of America through any screen sharing technology such as Remote Desktop Protocol (ware Remote Console ("VMRC")), or other current or future protocols designed to provide similar functionality.
- iii) In no event shall Vendor, without Customer's prior written approval, provide PHI received from, created, or received by Vendor on behalf of Customer to any employee or agent, including a subcontractor, if such employee, agent, or subcontractor receives, processes, or otherwise has access to the PHI outside of the United States.

**c) Third-Party Management**

- i) Vendor shall conduct risk assessments and reviews upon all third-parties with access to PHI no less than once per year. A summary of such assessment methodology, along with a summary of results, shall be provided to Customer upon written request.

**d) Remote Computing Requirements**

- i) Vendor shall require AAL2 ("Strong") authentication or AAL3 ("Multi-Factor") authentication as defined by the National Institute of Standards and Technology ("NIST") Special Publication 800-63-3 for all remote access to systems containing Customer Confidential Information.
- ii) In no case shall Vendor permit access to systems containing PHI from non-Vendor owned and controlled computing platforms including, but not limited to, employee owned computers, public computers, etc.

**e) Mobile Device Security**

- i) Vendor shall not permit Vendor Representatives to access PHI via any unencrypted mobile device including, but not limited to, unencrypted smartphones, unencrypted tablet computing devices, or any other unencrypted mobile device.
- ii) Vendor shall install a Mobile Device Management ("MDM") solution on all devices which may allow email which may contain PHI. Such solution shall be configured to encrypt and segregate such data from all other data. It shall furthermore be configured to allow remote wiping of the data in the event of theft or loss.

**f) Network Security**

- i) Vendor shall implement system, processes, or procedures to prevent the installation of and provisioning of IP addresses to unauthorized equipment on Vendor networks upon which PHI is processed or stored.

**g) Encryption Requirements**

- i) Vendor shall implement full disk encryption on any built-in or removable storage media in any Vendor controlled Personal Computer, portable computer, or any other personal computing device which may access, store, process, transmit, or create PHI. All such encryption shall minimally meet the Advanced

Encryption Standard with a 256-bit cypher key (“AES-256”) as outlined in the Federal Information Processing Standards Publication 197 (“FIPS 197”).

- ii) Vendor shall encrypt all PHI stored on Vendor servers, or other mass storage devices, even if those servers and devices are contained within a secured, hardened data center (data-at-rest encryption). Such encryption shall minimally meet the following requirements:
  - (1) Encryption Key Length—minimum key size 256 bits.
  - (2) Strong or Dual-Control Master Encryption Key Management.
  - (3) FIPS 140-2 Certified Cryptographic modules and encryption algorithms consistent with Cryptographic Module Validation Program (CMVP) and the National Institute of Standards and Technology (NIST) Special Publication 800-111 (AES).
- iii) Vendor shall encrypt all PHI placed on any removable storage device or media by Vendor per the above standard.
- iv) All encryption covered under this ISA shall comply with the following minimum standards:
  - (1) Cryptography and cryptographic algorithm use should be limited to technology that has undergone public scrutiny and review by reputable agencies.
  - (2) The date the cryptography and cryptographic algorithms were acquired should be retained in application or other appropriate documentation.
  - (3) For systems that are engaged in financial transactions only those algorithms and key lengths documented in ANSI X9 may be used. In all other cases, only algorithms and key lengths approved by the National Institute of Standards and Technology (NIST) in the Cryptographic Module Validation Program (CMVP) or Cryptographic Algorithm Validation Program (CAVP) may be used. It is required that tested and available encryption Application Program Interfaces (APIs) or other Vendor supplied and tested modules be used instead of creating an algorithm or using an unapproved and/or untested algorithm.
- v) Encryption and/or decryption keys must be adequately secured and only those trusted associates who have a “need to know” shall be given access to them. Vendor shall dispose of all storage media containing PHI, including those found in Multi-Function Devices, by purge (“Purge”) or destroy (“Destroy”) as those terms are defined in the NIST Special Publication 800-88, per all standards therein. Vendor shall maintain copies – either physical or electronic – of Certificate of Sanitization for a period of not less than three (3) years.
- vi) Vendor shall dispose of all paper media containing PHI via cross cut shredding resulting in pieces not to exceed ½” x ½”. In no case shall materials containing PHI be disposed of in general waste or recycle containers.

**h) Vulnerability Management**

- i) Vendor shall implement an Enterprise Vulnerability Management (“EVM”) solution for all devices connected to the Vendor’s LAN. Such solutions shall be designed to regularly scan the Vendor’s entire network for known vulnerabilities as related to the services authorized under Agreement.

**i) Incident and Breach Response and Preparedness**

- i) Any Computer Security Breach or Security Incident involving PHI shall be reported in accordance with the provisions of the Business Associate Agreement.
- ii) Vendor shall annually conduct an Incident exercise which includes, but is not limited to, a mock ransomware attack, risk analysis, and response.

**4. Provisions applicable to Vendors who handle PCI DSS covered data (“Cardholder Data”) – In addition to Section 2 above, the provisions in this section are applicable to Vendors who handle or process Cardholder Data.**

- a) Vendor shall protect Cardholder Data that the Vendor knowingly possesses according to requirements of the then current PCI DSS. Vendor agrees that it is responsible for the security of Cardholder Data that it possesses, including the functions relating to storing, processing, and transmitting of the Cardholder Data.
- b) Vendor affirms that, as of the effective date of this ISA, it has complied with all applicable requirements to be considered PCI DSS compliant, and has performed the necessary steps to validate its compliance with the PCI DSS.
- c) Vendor agrees to supply the current status of Vendor’s PCI DSS compliance status, and evidence of its most recent validation of compliance, to Customer upon execution of this ISA. Vendor must supply to Customer a new status report and evidence of validation of compliance at least annually.
- d) Vendor shall immediately notify Customer if it learns that it is no longer PCI DSS compliant and shall immediately provide Customer the steps being taken to remediate the non-compliance status. In no event should Vendor’s notification to Customer be later than seven (7) calendar days after Vendor learns it is no longer PCI DSS compliant.
- e) Vendor acknowledges that any indemnification provided for under the Agreement applies to the failure of the Vendor to be and to remain PCI DSS compliant.
- f) Vendor shall ensure that these requirements are cascaded to all downstream entities that may have access to Cardholder Data.

**g) Encryption Requirements**

- i) Vendor shall implement full-disk encryption on any built-in or removable storage media in any Vendor controlled Personal Computer, portable computer, or any other personal computing device which may access, store, process, transmit, or create Cardholder Data. All such encryption shall minimally meet the Advanced Encryption Standard with a 256-bit cypher key (“AES-256”) as outlined in the Federal Information Processing Standards Publication 197 (“FIPS 197”).
- ii) Vendor shall encrypt all Cardholder Data stored on Vendor servers or other mass storage devices, even if those servers and devices are contained within a secured, hardened data center (data at rest encryption). Such encryption shall minimally meet the aforementioned AES-256 requirement.
- iii) Vendor shall encrypt all Cardholder Data placed on any removable storage device or media by Vendor per the above standard.
- iv) Vendor shall ensure that all passwords are transmitted securely and encrypted when in storage. In the event that a hashing algorithm is used, Vendor must use a randomly-generated salt.
- v) All encryption covered under provision shall comply with the following minimum standards:
  - (1) Cryptography and cryptographic algorithm use should be limited to technology that has undergone public scrutiny and review by reputable agencies.
  - (2) The date the cryptography and cryptographic algorithms were acquired should be retained in application or other appropriate documentation.
  - (3) For systems that are engaged in financial transactions, only those algorithms and key lengths documented in ANSI X9 may be used. In all other cases, only algorithms and key lengths approved by the National Institute of Standards and Technology (NIST) in the Cryptographic Module Validation Program (CMVP) or Cryptographic Algorithm Validation Program (CAVP) may be

used. It is required that tested and available encryption Application Program Interfaces (APIs) or other vendor supplied and tested modules be used instead of creating an algorithm or using an unapproved and/or untested algorithm.

- (4) Encryption and/or Decryption keys must be adequately secured and only those trusted associates who have a “need to know” should be given access to them. Storage of these keys must be separate and distinct from the encrypted data. All compromised keys must be retired and replaced in a timely fashion.

**h) Secure Disposal**

- i) Vendor shall dispose of all storage media containing Cardholder Data, including those found in Multi-Function Devices, by purge (“Purge”) or destroy (“Destroy”) as those terms are defined in the NIST Special Publication 800-88, per all standards therein. Vendor shall maintain copies (either physical or electronic) of Certificate of Sanitization for a period of not less than three (3) years.
- ii) Vendor shall dispose of all paper media containing Cardholder Data via cross cut shredding resulting in pieces not to exceed ½” x ½”. In no case shall materials containing Cardholder Data be disposed of in general waste or recycle containers.

**5. Provisions applicable to Vendors who are providing services that include a Mobile Application (“Mobile App”) and/or a Web-Based Application (“Web App”) to Customer.**

- a) Vendor shall assure that all provided Mobile Applications comply with the following minimum security requirements:
  - i) Data shall not be stored unencrypted; this includes, but is not limited to, data stored in plist files, etc.
  - ii) Data shall be securely encrypted using a FIPS 140-2 encryption algorithm.
  - iii) Secure storage and use of keys.
  - iv) At the end of a session, all data and cache shall be securely deleted.
  - v) No preview screenshots or application tombstoning is in place.
  - vi) Application shall be configured to prevent cut/copy/paste functionality.
  - vii) Application shall be configured to prevent screenshots.
  - viii) Application shall be configured such that data is not exposed during the diagnostics and monitoring activities, e.g. Crashlytics.
- b) **Transmission Security**
  - i) TLS v1.2 or higher must be used in use for data transmission. In addition, iOS applications require App Transport Security (ATS) enabled, with no policy exceptions.
  - ii) Content Security Policy and security related HTTP headers set on endpoints.
- c) **Session Security**
  - i) Access to application requires authentication. Such authentication must not be able to be bypassed, this includes TouchID or similar functionality. Multifactor authentication may be required depending on the app and data sensitivity, e.g. TouchID with PIN.
  - ii) Application session must be set to time out in no more than fifteen (15) minutes.

- iii) When the session times out or the user logs out, the session must be terminated on both the client and server.
- iv) Sensitive information stored in RAM must be cleared at session termination. This includes usernames, passwords, and other session identifiers.

**d) Testing**

- i) All Mobile and/or Web Apps shall be submitted to Customer and shall be subject to penetration testing by Customer's Enterprise Information Protection ("EIP") Assurance Team. Such submission, if applicable, shall include the Mobile App build (.ipa or .apk file), API endpoints, and web application components.
- ii) EIP Assurance Team will additionally evaluate the application security program of the Mobile and/or Web App vendor/developer to include secure development lifecycle and the vendor/developer's in-house and third party security testing programs.
- iii) At the discretion of Customer EIP Assurance team, Customer may forgo in-house testing provided Vendor can provide evidence of the following:
  - (1) the Mobile and/or Web App and associated components (API and web application) underwent a recent third party penetration test that was conducted by a reputable firm; and
  - (2) the categories of vulnerabilities that were tested for; and
  - (3) Remediation of findings is complete.
- iv) Customer shall have the right to retest the Mobile and/or Web App for each release of the app at the sole discretion of Customer.

**6. Provisions applicable to Vendors who will have Humana software ("Customer Provided Software") installed on Vendor equipment.**

- a) Vendor shall use the Customer-Provided Software as directed by Customer and as necessary for provision of services to Customer and only during the term of the services engagement as reflected on a fully-executed, authorizing document.
- b) Vendor shall establish, maintain, and periodically provide to Customer a list of workstations upon which the Customer-Provided Software is installed, the serial number of each workstation, the full name of the Vendor Representative in control of each of those workstations, and the Customer User ID assigned to each of those Vendor Representatives. Vendor shall keep the above described information current and provide the information to Customer promptly upon request.
- c) Upon request by Customer, or upon termination of the provision of Services for any reason, Vendor shall promptly remove the Customer-Provided Software and provide attestation to Customer that the removal has been completed. Vendor shall not retain any copies of the Customer-Provided Software.
- d) Upon the removal of any Vendor Representative, in control of any workstation upon which Customer-Provided Software has been installed, from provision of Services to Customer for any reason, including separation from Vendor, Vendor shall promptly remove the Customer-Provided Software and provide attestation to Customer that the removal has been completed. Vendor shall not retain any copies of the Customer Provided Software.
- e) Customer may elect to provide remote support for Vendor Representatives using Customer Provided Software. Such support will be limited to addressing issues with the use of the Customer Provided Software in support of the Services. Vendor shall hold Customer harmless from any claim for loss or damages arising from or otherwise related to any such provision of support by Customer.

- f) Vendor understands that in the event Customer installs or provides for installation upon a Vendor workstation an information security agent, that agent will provide such information to Customer as is necessary for Customer to monitor the environment supporting the Services, including end-point analysis data, detailed logs of security events, etc.

**7. Section reserved for customized service requirements (e.g., identified deficiencies which need remediation).**

**IN WITNESS HEREOF**, the parties hereto, each acting under due and proper authority, have caused this ISA to be signed by their authorized representatives to be effective as of the Effective Date.

**BY CUSTOMER:**

**BY VENDOR:**

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Date)

\_\_\_\_\_  
(Date)

\_\_\_\_\_  
(Printed Name)

\_\_\_\_\_  
(Printed Name)

\_\_\_\_\_  
(Title)

\_\_\_\_\_  
(Title)

## HIPAA BUSINESS ASSOCIATE AGREEMENT ATTACHMENT

THIS BUSINESS ASSOCIATE AGREEMENT ATTACHMENT (“BAA”) is entered into by and between **Insert Correct Humana Entity Name** on behalf of its affiliates that underwrite or administer health plans (hereinafter “**Humana**”) and **Enter the Name of the Provider or Delegate Here** (hereinafter “**Business Associate**”).

**WHEREAS, Humana and Business Associate** have entered into a Delegation of Services Addendum (Addendum) whereby **Business Associate** will be performing delegated services on behalf of **Humana** involving the exchange of Protected Health Information and Protected Information; and

**WHEREAS, Humana and Business Associate** desire to enter into a HIPAA compliant **Business Associate Agreement** to outline the responsibilities of the parties;

**NOW, THEREFORE,** in consideration of the promises and mutual covenants contained herein, the parties agree as follows:

### SCOPE OF AGREEMENT

- A. In conformity with the regulations at 45 C.F.R. Parts 160-164 (the “Privacy and Security Rules”), **Humana** will provide **Business Associate** with access to, or have **Business Associate** create, maintain, transmit and/or receive certain Protected Health Information (“PHI” as defined below), thus necessitating a written agreement that meets the applicable requirements of the Privacy and Security Rules under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”) and the American Recovery and Reinvestment Act of 2009 (“ARRA”).
- B. **Humana and Business Associate** intend to protect the privacy and provide for the security of PHI disclosed to **Business Associate** pursuant to this BAA in compliance with HIPAA and the regulations promulgated thereunder by the U.S. Department of Health and Human Services, including, but not limited to, Title 45, Section 164.504(e) of the Code of Federal Regulations (“CFR”), as the same may be amended from time to time and other applicable state and federal laws, rules and regulations regarding privacy and security of personal information.
- C. The parties acknowledge that state and federal laws relating to electronic data security and privacy are rapidly evolving and that further amendment of this BAA may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of HIPAA, ARRA, and other applicable state and federal laws relating to the security or confidentiality of PHI.
- D. In the event of any conflict between this BAA and the Addendum as to the subject matter referenced herein, this BAA shall control.
- E. In consideration of the mutual promises below and the exchange of information pursuant to this BAA, the parties agree as follows:
  1. Definitions. The following terms shall have the meaning set forth below:
    - a. ARRA. “ARRA” means the American Recovery and Reinvestment Act of 2009
    - b. Business Associate. “Business Associate” shall mean Enter the Name of the Provider or Delegate Here acting as a Business Associate as such term is defined in 45 C. F. R. 160.103.
    - c. C. F. R. “C.F. R.” means the Code of Federal Regulations.
    - d. Designated Record Set. “Designated Record Set” has the meaning assigned to such term in 45 C. F. R. 164.501.

- e. Discovery. “Discovery” shall mean the first day on which a Security Breach is known to **Business Associate** (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of **Business Associate**), or should reasonably have been known to **Business Associate**, to have occurred.
- f. Electronic Health Record. “Electronic Health Record” means an electronic record of health-related information on an individual that is created, gathered, managed and consulted by authorized health care clinicians and staff.
- g. Electronic Protected Health Information. “Electronic Protected Health Information” means information that comes within paragraphs 1 (i) or 1 (ii) of the definition of “Protected Health Information”, as defined in 45 C. F. R. 160.103.
- h. Individual. “Individual” shall have the same meaning as the term “individual” in 45 C. F. R. 164.501 and 45 C. F. R. 160.103 and shall include a person who qualifies as personal representative in accordance with 45 C. F. R. 164.502 (g)(1).
- i. Protected Health Information. “Protected Health Information” or “PHI” shall have the same meaning as the term “Protected Health Information”, as defined by 45 C. F. R. 160.103, limited to the information created or received by **Business Associate** from or on behalf of Humana.
- j. Required by Law. “Required by Law” shall have the same meaning as the term “required by law” in 45 C. F. R. 164.501 and 45 C. F. R. 160.103.
- k. Secretary. “Secretary” shall mean the Secretary of the Department of Health and Human Services or his/her designee.
- l. Security Breach. “Security Breach” means the unauthorized acquisition, access, use or disclosure of Protected Health Information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. Security Breach does not include:
  - i. any unintentional acquisition, access, or use of Protected Health Information by an employee or individual acting under the authority of **Business Associate** if:
    - I. such acquisition, access or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with **Business Associate**; and
    - II. such information is not further acquired, accessed, used or disclosed by any person; or
  - ii. any inadvertent disclosure from an individual who is otherwise authorized to access Protected Health Information at a facility operated by **Business Associate** to another similarly situated individual at the same facility; and
  - iii. any such information received as a result of such disclosure is not further acquired, accessed, used or disclosed without authorization by any person.
- m. Security Incident. “Security Incident” shall have the same meaning as the term “security incident” in 45 C. F. R. 164.304.
- n. Standard Transactions. “Standard Transactions” means the electronic health care transactions for which HIPAA standards have been established, as set forth in 45 C. F. R., Parts 160 and 162.

- o. Subcontractor. “Subcontractor means a business associate as defined by the HIPAA privacy rule that creates, receives, maintains, or transmits Protected Health Information on behalf of another business associate.
- p. Terms. All other terms used, but not defined, shall have the same meaning as those terms are given in 45 C.F.R. 160-164.
- q. Unsecured Protected Health Information. “Unsecured Protected Health Information” shall have the meaning as the term “unsecured protected health information in 45 C.F.R. 164.402.

2. Obligation of Business Associate.

- a. Permitted Uses and Disclosures. **Business Associate** may create, use and/or disclose Humana Member’s PHI pursuant to the Addendum or this only in accordance with the specifications set forth in the underlying Addendum, this BAA or as Required by Law provided that such use or disclosure would not violate the Privacy and Security Rules if done by Humana or the minimum necessary policies and procedures of Humana.
- b. Specific Use and Disclosure Provisions
  - i. Except as otherwise prohibited by this BAA, **Business Associate** may use Protected Health Information for the proper management and administration of the **Business Associate** or to carry out the legal responsibilities of the **Business Associate**.
  - ii. Except as otherwise prohibited by this BAA, **Business Associate** may disclose Protected Health Information for the proper management and administration of the **Business Associate**, provided that disclosures are Required By Law, or **Business Associate** obtains reasonable assurances, in the form of a business associate agreement, from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the **Business Associate** of any instances of which it is aware in which the confidentiality of the information has been breached in accordance with the Security Breach and Security Incident notifications requirements of this BAA.
  - iii. **Business Associate** shall not directly or indirectly receive remuneration in exchange for any Protected Health Information of an Individual without Humana’s prior written approval and notice from Humana that it has obtained from the individual, in accordance with 45 C.F.R. 164.508, a valid authorization that includes a specification of whether the Protected Health Information can be further exchanged for remuneration by **Business Associate**. The foregoing shall not apply to Humana’s payments to Business Associate for services delivered by **Business Associate** to Humana.
  - iv. Except as otherwise prohibited by this BAA, **Business Associate** may use Protected Health Information to provide data aggregation services to Humana as permitted by 42 C.F.R. 164.504(e)(2)(i)(B).
  - v. **Business Associate** may use Protected Health Information to report violation of law to appropriate Federal and State authorities, consistent with 164.502 (j)(1).
  - vi. **Business associate** may not use or disclose Protected Health Information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity except for the specific uses and disclosures set out above in this Section 2.(b).
- c. **Business Associate** agrees to document such disclosures of Protected Health Information as would be required for **Humana** to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. 164.528.

- d. **Business Associate** agrees to provide to **Humana**, in the time and manner designated by **Humana**, the information collected in accordance with this BAA, to permit **Humana** to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. 164.528. In addition, with respect to information contained in an Electronic Health Record, **Business Associate** shall document, and maintain such documentation for three (3) years from date of disclosure if such disclosures as would be required for **Humana** to respond to a request by an Individual for an accounting of disclosures of information contained in an Electronic Health Record, as required by Section 13405(c) of Subtitle D (Privacy) of ARRA and related regulations issued by the Secretary from time to time.
- e. Nondisclosure. **Business Associate** agrees to not use or disclose Protected Health Information other than as permitted or required by this BAA or as Required By Law. **Business Associate** shall also comply with any further limitations on uses and disclosures agreed to by **Humana** in accordance with 45 C.F.R. 164.522 provided that such agreed upon limitations have been communicated to **Business Associate** in accordance with Section 3(d) of this BAA.
- f. Reporting of Disclosures and Mitigation. **Business Associate** shall provide immediate written notice to **Humana** of any use or disclosure of PHI other than as specifically provided for by the Addendum or this BAA. Such notice shall be provided in the manner set out at Paragraph 2(l) of this BAA. **Business Associate** agrees to mitigate, to the extent practicable, any harmful effect that is known to **Business Associate** of a use or disclosure of Protected Health Information by **Business Associate** in violation of the requirements of this BAA.
- g. **Business Associate** shall report to **Humana** any Security Incident of which it becomes aware. For purposes of reporting to **Humana**, any attempted unsuccessful Security Incident means any attempted unauthorized access that prompts **Business Associate** to investigate the attempt or review or change its current security measures.
- h. Safeguards. **Business Associate** shall use appropriate safeguards to prevent use or disclosure of Protected Health Information other than as specifically provided for by the Addendum or this BAA. Such safeguards shall at a minimum include: (i) a comprehensive written information privacy and security policy; and (ii) a program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the **Business Associate's** operations and the nature and scope of his/her/its activities; and (iii) periodic and mandatory privacy and security training and awareness to its employees and Subcontractors; and (iv) appropriate confidentiality agreements with all employees, Subcontractors, independent contractors and any entity to which **Business Associate** has delegated or sub-delegated his/her/its rights, duties, activities and/or obligations under the Addendum or this BAA which contain terms and conditions that are the same or similar to those contained in this BAA.
- i. **Business Associate** acknowledges that it shall request from **Humana** and so disclose to its affiliates, agents and Subcontractors or other third parties, (i) the information contained in a "limited data set," as such term is defined at 45 C.F.R. 164.514(e)(2), or, (ii) if needed by **Business Associate**, to the minimum necessary to accomplish the intended purpose of such requests or disclosures. In all cases, **Business Associate** shall request and disclose Protected Health Information only in a manner that is consistent with guidance issued by the Secretary from time to time
- j. With respect to Electronic Protected Health Information, **Business Associate** shall implement and comply with (and ensure that its Subcontractors implement and comply with) the administrative safeguards set forth at 45 C.F.R. 164.308, the physical safeguards set forth at 45 C.F.R. 164.310, the technical safeguards set forth at 45 C.F.R. 164.312, and the policies and procedures set forth at 45 C.F.R. 164.316 to reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains, or transmits on behalf of **Humana**.

- k. With respect to Electronic Protected Health Information, **Business Associate** shall ensure that any agent, including a Subcontractor, to whom it provides Electronic Protected Health Information, agrees to implement reasonable and appropriate safeguards to protect it.
- l. Notification of Breach. **Business Associate** shall report to **Humana** any potential Security Breach of Unsecured Protected Health Information without unreasonable delay and in no case later than five (5) calendar days after Discovery of a Security Breach. Such notice shall include: (i) the identification of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by **Business Associate**, to have been, accessed, acquired, or disclosed; and (ii) a brief description of the event; and (iii) the date of the potential Security Breach; and (iv) the date of discovery; and (v) the type of Protected Health Information involved; and (vi) any preliminary steps taken to mitigate the damage; and (vii) a description of any investigatory steps taken. In addition, **Business Associate** shall provide any additional information reasonably requested by Humana for purposes of investigating the Security Breach. **Business Associate's** notification of a Security Breach under this section shall comply in all respects with each applicable provision of Section 13400 of Subtitle D (Privacy) of ARRA and related guidance issued by the Secretary from time to time.
- i. Breach notifications must be reported to Humana by one of the following methods:
- By Mail:** Humana Privacy Officer  
500 West Main Street, 26<sup>th</sup> Floor  
Louisville, KY 40202
- By Phone:** 502-580-3700
- By email:** privacyoffice@humana.com
- m. In addition to the foregoing, **Business Associate** agrees that in the event of such a notification set forth in Section 2(k), Humana shall have the sole right to determine (i) whether notice is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, media outlets and/or HHS, or others as required by law or regulation, or in **Humana's** discretion; and (ii) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation. Any such notice or remediation shall be at **Business Associate's** sole cost and expense.
- n. Availability of Information. **Business Associate** agrees to provide access, at the request of **Humana**, and in the time and manner designated by **Humana**, to Protected Health Information in a Designated Record Set, to Humana or, as directed by **Humana**, to an Individual in order to meet the requirements under 45 C.F.R. 164.524. Humana's determination of what constitutes "Protected Health Information" or a "Designated Record Set" shall be final and conclusive. If **Business Associate** provides copies or summaries of Protected Health Information to an Individual it may impose a reasonable, cost-based fee in accordance with 45 C.F.R. 164.524 (c)(4).
- o. Amendment of PHI. **Business Associate** shall make PHI available to **Humana** as reasonably required to fulfill **Humana's** obligations to amend such PHI pursuant to HIPAA and the HIPAA Regulations, including, but not limited to, 45 CFR Section 164.526 and **Business Associate** shall, as directed by Humana, incorporate any amendments to PHI into copies of such PHI maintained by **Business Associate**.
- p. Data Aggregation Services. For purposes of this Section, "Data Aggregation" means, with respect to **Humana's** PHI, the combining of such PHI by **Business Associate** with the PHI received by **Business Associate** in its capacity as a **Business Associate** of another covered entity, as that term is defined under HIPAA to permit data analyses that relate to the health care operations of the respective Covered Entities. If applicable, **Business Associate** shall provide the following Data Aggregation services relating to the health care operations of **Humana**, as such **Business Associate** shall comply with

restrictions on the use and disclosure of PHI. **Humana** shall notify **Business Associate** of such restrictions upon the effective date of this BAA.

- i. Outcomes data aggregation
- ii. Profiling of utilization patterns, outcomes and prescribing patterns of providers
- iii. Geographic profiling of patterns of care rendered to Humana Members

- q. Subcontractors. **Business Associate** shall maintain written agreements with Subcontractors, as necessary to perform the services required under the Addendum, in a form consistent with, the terms and conditions, restrictions and requirements established in this BAA. The business associate agreements shall require such Subcontractors to enter into additional downstream business associate agreements in order for **Business Associate** to comply with this BAA and **Business Associate's** independent HIPAA obligations as set out in 45 C.F.R. 164.502(e)(1)(ii) and 164.308(b)(2). Sample copies of the standard business associate agreements between **Business Associate** and Subcontractors will be made available upon request. In the event of any conflict between this BAA and any agreement between **Business Associate** and any Subcontractor, the requirements in this BAA shall control. **Business Associate** agrees to notify **Humana** of any material change(s) to the aforementioned business associate agreements at least thirty (30) days prior to implementing such change(s). **Business Associate** shall ensure that any agents, including Subcontractors, to whom it provides **Humana** Member's PHI received from, created by, or received by **Business Associate** on behalf of **Humana**, agrees to the same restrictions and conditions that apply to **Business Associate** with respect to such PHI. In no event shall **Business Associate**, without **Humana's** prior written approval, provide Protected Health Information received from, or created or received by **Business Associate** on behalf of **Humana**, to any employee or agent, including a Subcontractor, if such employee, agent or Subcontractor receives, processes or otherwise has access to the Protected Health Information outside of the United States.
- r. Internal Practices. **Business Associate** agrees to make (i) internal practices, books, and records, including policies and procedures, relating to the use and disclosure of Protected Health Information received from, or created or received by **Business Associate** on behalf of, **Humana**, and (ii) policies, procedures, and documentation relating to the safeguarding of Electronic Protected Health Information available to **Humana**, or directly to the Secretary, in a time and manner designated by **Humana** or the Secretary, as applicable, for purposes of the Secretary determining **Humana's** compliance with the Privacy and Security Rules.
- s. If **Business Associate** conducts any Standard Transactions on behalf of **Humana**, **Business Associate** shall comply with the applicable requirements of 45 C.F.R. Parts 160-162.
- t. During the term of this BAA, **Business Associate** may be asked to complete a security survey and/or attestation document designed to assist **Humana** in understanding and documenting **Business Associate's** security procedures and compliance with the requirements contained herein. **Business Associate's** failure to complete either of these documents within the reasonable timeframe specified by **Humana** shall constitute a material breach of this BAA.

3. Obligations of Humana.

- a. **Humana** will use appropriate safeguards to maintain the confidentiality, privacy and security of PHI in transmitting same to **Business Associate** pursuant to the Addendum and this BAA.
- b. **Humana** shall notify **Business Associate** of any limitation(s) in **Humana's** notice of privacy practices that **Humana** produces in accordance with 45 C.F.R. 164.520 (as well as any changes to that notice), to the extent that such limitation(s) may affect **Business Associate's** use or disclosure of Protected Health Information.

- c. **Humana** shall provide **Business Associate** with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes affect **Business Associate's** use or disclosure of Protected Health Information.
    - d. **Humana** shall notify **Business Associate** of any restriction to the use or disclosure of Protected Health Information that Humana has agreed to in accordance with 45 C.F.R. 164.522, to the extent that such restriction may affect **Business Associate's** use or disclosure of Protected Health Information.
  4. Audits, Inspection and Enforcement. From time to time upon reasonable advance notice, or upon a reasonable determination by **Humana** that **Business Associate** has potentially or actually breached this BAA, **Humana** may inspect the facilities, systems, books, procedures and records of **Business Associate** to monitor compliance with this BAA. **Business Associate** shall promptly remedy any violation of any term of this BAA and shall certify the same to **Humana** in writing.
    - a. To the extent that **Humana** determines that such examination is necessary to comply with **Humana's** legal obligations pursuant to HIPAA relating to certification of its security practices, **Humana** or its authorized agents or Subcontractors, may, at **Humana's** expense, examine **Business Associate's** facilities, systems, procedures and records as may be necessary for such agents or Subcontractors to certify to **Humana** the extent to which **Business Associate's** administrative, physical and technical safeguards comply with HIPAA, the HIPAA Regulations or this BAA.
  5. Waiver. Waiver, whether expressed or implied, of any breach of any provision of this BAA shall not be deemed to be a waiver of any other provision or a waiver of any subsequent or continuing breach of the same provision. In addition, waiver of one of the remedies available to either party in the event of a default or breach of this BAA by the other party, shall not at any time be deemed a waiver of a party's right to elect such remedy(ies) at any subsequent time if a condition of default continues or recurs.
  6. Termination.
    - a. Term. The provisions of this BAA shall take effect on the BAA's Effective Date and shall terminate when all of the Protected Health Information provided by **Humana** to **Business Associate**, or created, maintained, transmitted or received by **Business Associate** on behalf of **Humana**, is destroyed or returned to **Humana**, or, retained in accordance with Section 6(c)(ii) below.
    - b. Termination for Cause. Without limiting the termination rights of the parties pursuant to the BAA and upon, either party's knowledge of a material breach of this BAA by the other party, the non-breaching party shall provide an opportunity for the breaching party, to cure the breach or end the violation, or terminate the BAA, if the breaching party does not cure the breach or end the violation within the time specified by the non-breaching party, or immediately terminate this BAA, if, in the non-breaching party's reasonable judgment cure is not possible.
    - c. Effect of Termination.
      - i. Except as provided in Section 6(d), upon termination of this BAA, for any reason, **Business Associate** shall return or destroy all Protected Health Information received from **Humana**, or created, maintained, transmitted or received by **Business Associate** on behalf of **Humana**. This provision shall apply to Protected Health Information that is in the possession of Subcontractors or agents of **Business Associate**. **Business Associate** shall retain no copies of the Protected Health Information.
      - ii. In the event the **Business Associate** determines that returning or destroying the Protected Health Information is infeasible, **Business Associate** shall provide to **Humana** notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the parties that return or destruction of Protected Health Information is infeasible, per Section 6(a) above, **Business Associate** shall continue to extend the protection of this BAA to such Protected

Health Information and limit further uses and disclosures of such Protected Health Information for so long as **Business Associate** maintains such Protected Health Information.

- d. Upon termination of this BAA for any reason, **Business Associate**, with respect to Protected Health Information received from Humana, or created, maintained, or received by **Business Associate** on behalf of Humana, shall:
  - i. Retain only that Protected Health Information which is necessary for **Business Associate** to continue its proper management and administration or to carry out its legal responsibilities;
  - ii. Return to Humana the remaining Protected Health Information that the **Business Associate** still maintains in any form;
  - iii. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to Electronic Protected Health information to prevent use or disclosure of the Protected Health Information, other than as provided for in this Section, for as long as **Business Associate** retains the Protected Health Information;
  - iv. Not use or disclose the Protected Health Information retained by **Business Associate** other than for the purposes for which such Protected Health Information was retained and subject to the same conditions set out in Section 2(b) under "Permitted Uses and Disclosures By Business Associate" which applied prior to termination; and
  - v. Return to **Humana** or destroy the Protected Health Information retained by **Business Associate** when it is no longer needed by **Business Associate** for its proper management and administration or to carry out its legal responsibilities.
- e. Judicial or Administrative Proceedings. Either party may terminate the Addendum, effective immediately, if: (i) the other party is named as a defendant in a criminal proceeding for a violation of HIPAA or (ii) a finding or stipulation that the other party has violated any standard or requirement of HIPAA or other security or privacy laws is made in any administrative or civil proceeding in which the party has been joined.
7. Indemnification. **Humana** and **Business Associate** will indemnify hold harmless and defend the other party to this BAA from and against any and all claims, losses, liabilities, costs and other expenses incurred as a result of, or arising directly or indirectly out of or in connection with: (i) any misrepresentation, breach of warranty or non-fulfillment of any undertaking on the part of the party under this BAA; and (ii) any claims, demands, awards, judgments, actions and proceedings made by any person or organization arising out of or in any way connected with the party's performance under this BAA.
8. Disclaimer. **Humana** makes no warranty or representation that compliance by **Business Associate** with this BAA, HIPAA or ARRA will be adequate or satisfactory for **Business Associate's** own purposes or that any information in **Business Associate's** possession or control, or transmitted or received by **Business Associate**, is or will be secure from unauthorized use or disclosure. Business Associate is solely responsible for all decisions made **by Business Associate** regarding the safeguarding of PHI.
9. Assistance in Litigation or Administrative Proceedings. **Business Associate** shall make itself, and any Subcontractors, employees or agents assisting **Business Associate** in the performance of its obligations under the Addendum, available to **Humana**, at no cost to **Humana**, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against **Humana**, its directors, officers or employees based upon claimed violation of HIPAA, the HIPAA Regulations or other laws relating to security and privacy, except where **Business Associate** or its Subcontractor, employee or agent is a named adverse party.

- 10. No Third Party Beneficiaries. The parties have not created and do not intend to create by this BAA any third party rights under this BAA, including but not limited to Members. There are no third party beneficiaries to this BAA.
- 11. Receipt of PHI. **Business Associate's** receipt of **Humana** Member's PHI pursuant to the transactions contemplated by the Addendum shall be deemed to begin on the execution date below, and **Business Associate's** obligations under this BAA shall commence with respect to such PHI upon such receipt.
- 12. Interpretation. The parties agree that any ambiguity in this BAA shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HIPAA Regulations.
- 13. Regulatory References. A reference in this BAA to a section in the Privacy and Security Rules means the section as in effect or as amended.
- 14. Amendment. Upon the enactment of any law or regulation affecting the use or disclosure of Protected Health Information, the safeguarding of Electronic Protected Health Information, or the publication of any decision of a court of the United States or any state relating to any such law or the publication of any interpretive policy or opinion of any governmental agency charged with the enforcement of any such law or regulation, the party's shall negotiate in good faith to amend this **Business Associate** agreement to bring it into compliance such new law, regulation or decision of the court. If the parties are unable to agree on an amendment within thirty (30) days thereafter, then either of the parties may terminate the BAA on thirty (30) days written notice to the other party.
- 15. Survival. The respective rights and obligations of **Business Associate** under Sections 6 and 7 of this BAA shall survive the termination of this Addendum.
- 16. Governing Law. This BAA shall be governed by and construed in accordance with the laws of the Commonwealth of Kentucky.

**Address for Notice:**

---



---



---



---

**Address for Notice:**

---



---



---



---

**COPY TO:**

Humana Inc.  
 500 West Main Street  
 Louisville, KY 40202  
 Attn: Law Department

**COPY TO**

---



---



---



---

**DELEGATED CREDENTIALING**  
**NO PROTECTED HEALTH INFORMATION CERTIFICATION ATTACHMENT [CREDENTIALING ONLY]**

**Insert Delegate Name Here (Delegate)** performs credentialing on behalf of **Insert Humana Entity Name** here (**“Delegator”**) under a Delegation Services Addendum (Addendum). **Delegate** certifies that it does not receive any Protected Health Information (“PHI”), as that term is defined under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 (“HIPAA”), nor uses any PHI to perform the duties delegated under the Addendum.

As a result, **Delegate** believes and hereby represents to **Delegator** that the HIPAA Privacy regulations do not require **Delegate** to enter into a Business Associate Agreement with **Delegator** at this time.

**Delegate** understands and represents and warrants to **Delegator** that if **Delegate** must use or receive any PHI for any future delegated credentialing activities, **Delegate** will promptly notify **Delegator** prior to performing those activities so that **Delegate** and **Delegator** may enter into a Business Associate Agreement.

Delegate Signature:

---

Printed Name of Representative:

---

Representative Title:

---

Date:

---