GLOBALHEALTH, INC. & AFFILIATED COMPANIES
CONSUMER AUTHORIZATION AND RELEASE

In connection with **GLOBALHEALTH, INC. & AFFILIATED COMPANIES** considering me for Employment/agent, continued employment/agent, promotion or reassignment, I authorize **GLOBALHEALTH, INC. & AFFILIATED COMPANIES** and or its agent, ACCUFAX Div., Southvest Inc. to obtain a consumer report, criminal background check report, motor vehicle records, workers compensation records or investigative consumer report which may include information on my character, general reputation, personal characteristics, and mode of living from public record sources or through personal interviews with previous employers or associates. When requested by an employer motor vehicle records or a driving history may be obtained.

I authorize, without reservation, any person or entity contacted by **GLOBALHEALTH, INC. & AFFILIATED COMPANIES,** or its agent, ACCUFAX Div., Southvest Inc. to furnish the above-stated information, and I release any such person or entity from any and all liability for furnishing such information. I further release **GLOBALHEALTH, INC. & AFFILIATED COMPANIES**, its affiliated companies, their officers, employees and agents, and specifically, ACCUFAX Div., Southvest Inc., their affiliated companies, their officers, employees and agents from any liability and responsibility arising from the preparation of said report. I understand that false or misleading statements made on this authorization, or made during the employment/agent process, will disqualify me from consideration for employment/agent or result in my immediate discharge if employed.
By my execution hereof I acknowledge I have been provided with a separate Consumer Disclosure advising me that a report will be requested and used for the purpose of evaluating me for employment/agent, continued employment/agent, promotion, or reassignment as an employee.

PLEASE PRINT (Use Blue or Black Ink) **Requested by: 4052805656**

LEGAL NAME_____ DOB*_____ SS#_____

OTHER NAMES USED_____

DRIVERS LICENSE #_____ STATE ISSUED_____

Name exactly as it appears on Drivers License_____

CURR.

ADDR._____

CITY_____ ST_____ CO_____ ZIP_____ HOW LONG_____

PREV. ADDR._____

CITY_____ ST_____ CO_____ ZIP_____ HOW LONG_____

PREV. ADDR._____

CITY_____ ST_____ CO_____ ZIP_____ HOW LONG_____

Signature_____ Date_____

LIST ALL CITY/STATES RESIDED IN SINCE AGE 18 AND HOW LONG IN EACH CITY/STATE:

_____

APPLICANT COMPLETE INFORMATION BELOW (MAY WE CONTACT YOUR CURRENT EMPLOYER?) _ Y☐ __ N☐__

			From / To
Employer	City	Tel	Dates /
Employer	City	Tel	Dates /
Employer	City	Tel	Dates /

EDUCATION

Name	City,St	Tel	From / To
			Dates /

Most recent

Years attended Last year completed: 1 2 3 4 Degree(s)_____

Last name if different while in School_____

GLOBALHEALTH, INC. & AFFILIATED COMPANIES
CONSUMER AUTHORIZATION AND RELEASE

*** "Date of Birth" (DOB) or "Age" will be used solely for the purpose of identification in doing background checks and will not be considered or used for any other purpose.**

CONSUMER DISCLOSURE **(FCRA-1)**

In connection with **GLOBALHEALTH, INC. & AFFILIATED COMPANIES** considering you for employment/agent, continued employment/agent, promotion or reassignment, **GLOBALHEALTH, INC. & AFFILIATED COMPANIES** may obtain a consumer report, criminal background check report, motor vehicle report, workers compensation records or investigative consumer report on you which may include information on character, general reputation, personal characteristics, and mode of living from public record sources or personal interviews with previous employers or associates. You have the right, upon written request, to receive a written description of the nature and scope of the investigation requested and a written summary of your rights under the Fair Credit Reporting Act.

I HEREBY ACKNOWLEDGE RECEIPT:

_____ _____

PRINT NAME DATE

_____

SIGNATURE

Individual Agent Attestation

1) I, _____, accept appointment as an Agent to solicit and procure applications for GlobalHealth Holdings, LLC ("GlobalHealth") HMO products and understand and accept my responsibility to comply with all applicable State and Federal laws and GlobalHealth policies.

2) I agree to maintain licensure and complete mandatory training as required by the state of Oklahoma and the Centers for Medicare and Medicaid Services (CMS) (if applicable).

3) I understand that if I am non-compliant with the terms of the Field Marketing Organization Agreement, as amended from time to time, applicable State or Federal laws, regulations, policies, GlobalHealth instructions and/or the Business Associate Addendum between me and GlobalHealth, it may result in my termination as an agent, thereby prohibiting my ability to market or sell products on behalf of GlobalHealth.

4) I acknowledge and agree that my appointment authorizes me to sell GlobalHealth products solely within the service areas as GlobalHealth designates.

5) I agree to actively promote and market any and all insurance products required by GlobalHealth.

6) I agree that I will not promote or market GlobalHealth products until the completion of all training, testing, licensure and appointment, as required by GlobalHealth, is complete.

7) I will not use the trademarks or tradenames of GlobalHealth and shall not advertise using the name of GlobalHealth without the express written approval of GlobalHealth.

_____ _____

Signature Date

_____ _____

Date of Birth National Producer Number (NPN)

_____

Affiliated Field Marketing Organization

Broker/Producer/Agent Appointment Application Questionnaire

The Broker Appointment Application must be completed and returned, along with a copy of your current State of Oklahoma Insurance Department Accident & Health Agent license, to: Business Development:

GlobalHealth Holdings, LLC
210 Park Avenue, Ste 2800
Oklahoma City, OK 73102-5621

Individual/Sole Proprietor Applicant:

Applicant Full Name: _____
Date of Birth: _____ Social Security Number: _____
Business Address: _____
City: _____ State: _____ Zip: _____
County: _____ Business Phone Number: _____
Fax Number: _____ Email: _____
Agent License Number: _____

Corporate Applicant:

Corporation/Agency Full Name: _____
Taxpayer ID: _____ State of Incorporation: _____
Business Address: _____
City: _____ State: _____ Zip: _____
County: _____ Business Phone Number: _____
Fax Number: _____ Email: _____
Agent License Number(s): _____

1. Do you carry the required minimum Errors and Omissions Insurance Coverage as described in your Agreement:
   (Please attach the face page of your current policy.) Yes [ ] No [ ]

2. Have you ever been charge with or convicted of a felony? If yes, please explain. Yes [ ] No [ ]

   _____
   _____
   _____

3. Have you ever been fined, reprimanded, or sanctioned in any state for a violation of insurance laws, HMO regulations, or other administrative regulations, or refused a license to sell insurance in any state? If yes, please explain. Yes [ ] No [ ]

   _____
   _____
   _____

4. Have you ever been excluded, debarred, restricted, suspended, or sanctioned from participation in Medicare, Medicaid, CHAMPUS, or any other government-funded program? If yes, please explain. Yes [ ] No [ ]

5. If you are not a U.S. citizen, are you eligible to work in the U.S.?
   (Please attach proof of eligibility if applicable.) Yes [ ] No [ ] N/A [ ]

6. Are you a sole proprietor or independently licensed Producer/Agent qualified as a Producer/Agent for accident and health and/or HMO commercial products? If not, provide the legal entity business name, business address, contact person's name, title, and phone number at the contracted General Agent and/or Broker Agency in which you are employed or subcontracted for this appointment. Yes [ ] No [ ]

   _____
   _____
   _____

7. Please list other companies to which you have been appointed within the past five (5) years.

   _____
   _____
   _____
   _____
   _____

Consent and Release

By signing below, I affirm that the information I have submitted in my request for Producer/Agent appointment, along with any attachments or supplemental information, is true, current, and complete to the best of my knowledge. I understand that omissions or misrepresentations may result in denial of my request or immediate revocation of my appointment by GlobalHealth Holdings, LLC. I consent to such investigations and agree to interviews as GlobalHealth Holdings, LLC, may make regarding my background (including criminal and civil litigation records checks), previous employment, personal references, educational records, driving records, credit reports, and general character. I authorize the use of this information and any other information obtained in connection with my request for appointment. I authorize past employers, all references, and any other persons to answer all questions asked concerning my ability, character, reputation, previous education, employment records, and Producer/Agent licensure records. I release all such persons from any liability or damages from having furnished such information. I understand that I have certain rights under the FCRA and I hereby affirm that I have received and read the FCRA Disclosure Statement and my rights as a consumer in advanc3e of signing this form.

I understand that this form must be completed or I will be ineligible for appointment by GlobalHealth Holdings, LLC. This authorization will remain in effect throughout my initial appointment term and subsequent renewal appointment term(s) with GlobalHealth Holdings, LLC. A photocopy of this document shall be as effective as the original.

_____ _____

Producer/Agent Signature Date

_____ _____

Printed Full Name License Number

BUSINESS ASSOCIATE ADDENDUM

THIS BUSINESS ASSOCIATE ADDENDUM is effective on the Effective Date of the Underlying Agreement by and between GlobalHealth Holdings, LLC ("Company") and Agent ("Business Associate").

RECITALS

WHEREAS, Company and Business Associate have or are entering into the Individual Agent/Broker Agreement ("Underlying Agreement") pursuant to which Business Associate provides services to Company and, in connection with those services, Company may use and/or disclose to Business Associate certain protected health information ("PHI") that is subject to protection under privacy and security standards implemented pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended from time to time, and state or federal privacy laws or regulations (collectively the "Privacy/Security Standards"); and

WHEREAS, the parties desire to comply with the Privacy/Security Standards with respect to Company's enrollees/members; and

NOW THEREFORE, for and in consideration of the recitals above and the mutual covenants and conditions herein contained, Company and Business Associate enter into this Business Associate Addendum ("Addendum") to provide a full statement of their respective responsibilities.

SECTION 1 – DEFINITIONS

1.1 Definitions. Unless otherwise provided in Section 10 herein, capitalized terms shall have the same meaning as set forth in the HIPAA regulations, 45 C.F.R. §160-164.

SECTION 2 – OBLIGATIONS OF BUSINESS ASSOCIATE

2.1 Scope of Use of PHI. Business Associate shall not use PHI other than as expressly permitted by this Addendum, the Underlying Agreement, or as required or permitted by law. Unless otherwise limited herein, the Business Associate may use PHI (i) to perform its duties and legal obligations to Company pursuant to this Addendum and the Underlying Agreement, provided that such uses are permitted by law; and (ii) as necessary for purposes of managing its internal business processes relating to the functions under this Addendum or the Underlying Agreement. Business Associate agrees that it will limit its requests for PHI to the minimum necessary to permit it to carry out the services specified in the Underlying Agreement.

2.2 Disclosure of PHI. Unless otherwise limited herein, Business Associate may disclose the PHI to third parties for the purpose of fulfilling its duties and legal obligations pursuant to this Addendum if the Business Associate represents to Company, in writing, that (i) the Business Associate has received written assurances from the third party that the PHI will be held confidentially and used or further disclosed only as required or permitted by law or for the purposes for which it was disclosed to the third party; and (ii) the third party will notify Business Associate of any instances of which it becomes aware in which confidentiality has been breached. Business Associate agrees that it will limit its disclosure of

PHI to the minimum necessary to permit such third parties to carry out the services specified in the Underlying Agreement.

2.3 Use of Subcontractors. To the extent Business Associate uses one or more subcontractor or Agent to provide services under the Underlying Agreement, and such subcontractors or Agents receive or have access to PHI, Business Associate agrees that it will ensure that each such subcontractor or Agent shall agree, in writing, to all of the same restrictions and conditions to which Business Associate is bound. Business Associate shall disclose to its subcontractors or Agents only the minimum PHI necessary to perform or fulfill a specific function required or permitted under the Underlying Agreement or this Addendum.

2.4 Individual Rights Regarding Designated Record Sets. If Business Associate maintains a Designated Record Set on behalf of Company, Business Associate shall (i) permit the Individual to inspect or copy PHI contained in that set about the Individual under the conditions and limitations required under 45 C.F.R. §164.524, as amended from time to time; and (ii) amend PHI maintained by Business Associate as requested by Company. Business Associate shall respond to any request by Company for access by an Individual within seven (7) days of such request and shall make any amendment requested by Company within ten (10) days of such request. If Business Associate maintains a Designated Record Set, Business Associate shall accommodate an Individual's right to have access to PHI about the individual in a Designated Record Set in accordance with the Privacy/Security Standards set forth at 45 C.F.R. §164.526, as amended from time to time. Business Associate shall have a process in place for amendments and for appending such requests to the Designated Record Set.

2.5 Accounting of Disclosures. Business Associate shall make available to Company the information required for an accounting of disclosures of PHI with respect to an Individual. Such accounting is limited to disclosures that were made in the six (6) years prior to the request of the Individual and shall not include any disclosures prior to April 14, 2003. Business Associate shall provide a record of the disclosures of PHI made, including, but not limited to, the date of the disclosure, the name and, if known, the address of the recipient of the PHI, a brief description of the PHI disclosed, and the purpose of the disclosure. Business Associate shall make such record available to Company upon request, but in no event later than fifteen (15) days following receipt of the request. Such accounting shall be provided as long as Business Associate maintains PHI.

2.6 Safeguards for Protection of PHI. Business Associate agrees that it will use commercially reasonable and appropriate safeguards to prevent use or disclosure of PHI other than as permitted by this Agreement or required or permitted by law. Business Associate will implement and maintain appropriate policies and procedures to protect and safeguard the confidentiality and integrity of PHI. Business Associate shall provide Company with information concerning such safeguards as Company may from time to time request. Business Associate acknowledges that Company is relying on the security safeguards of Business Associate in selecting Business Associate as a business partner. Business Associate shall promptly notify the Company's Privacy Officer of any material change to any aspect of its security safeguards in violations of this Addendum or the Underlying Agreement by its officers, directors, associates, employees, volunteers, contractors or Agents. Business Associate shall be fully liable to Company and any affected individuals for any acts, failures, or omissions of Business Associate or its subcontractors as though they were its own acts, failures, or omissions.

2.7 Reporting of Unauthorized Use. Business Associate will promptly report to Company's Privacy Officer any unauthorized use or disclosure immediately upon becoming aware of it and shall

mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Addendum. If requested by Company, such report must be reduced to a written form. Business Associate shall permit Company to investigate any such report and to examine Business Associate's premises, records, and practices for the purpose of determining Business Associate's compliance with this Addendum.

2.8 Breach or Misuse of PHI. Business Associate recognizes that any breach of confidentiality or misuse of information found in and/or obtained from records may result in the termination of this Addendum, the Underlying Agreement and/or legal action. Business Associate further recognizes that certain breaches of PHI may be reportable under the Health Information Technology for Economic and Clinical Health ("HITECH") Act and that Business Associate may be liable for monetary penalties under HITECH.

2.9 Liability under Privacy Rule. Business Associate recognizes it may be held directly liable for uses and disclosures of PHI that are not in accord with the Privacy Rule or this Addendum. Further, Business Associate may be directly liable for (1) failing to disclose PHI when required by the Secretary to do so for the Secretary to investigate and determine compliance with the HIPAA Rules; (2) failing to disclose PHI to Company, individual, or individual's designee, as necessary to satisfy Company's obligations with respect to an individual's request for an electronic copy of PHI; (3) failing to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request; or (4) failing to enter into business associate agreements with subcontractors that create or receive PHI on its behalf.

2.10 Identity Theft Regulations. To the extent that Business Associate provides services in connection with the maintenance, billing, or collection of patient accounts for Company, Business Associate confirms that it has adopted and is implementing a program designed to detect, prevent, and mitigate the risk of identity theft in conformity with the requirements of the Red Flag Rules issued by the Federal Trade Commission, 16 C.F.R. Part 681. In addition, Business Associate shall: (1) report to Company any pattern, practice, or specific activity that indicates the possible existence of identity theft ("Red Flags") involving anyone associated with Company, including its Members, employees, Agents, and contractors, and (2) take appropriate steps to prevent or mitigate identity theft when a Red Flag is detected.

SECTION 3 – OBLIGATIONS OF COMPANY

3.1 Limitations in Notice of Privacy Practices. Company agrees to notify Business Associate of any limitations in the Notice of Privacy Practices that it provides to individuals pursuant to 45 C.F.R. §164.520, to the extent that such limitations may affect Business Associate's use or disclosure of PHI.

3.2 Withdrawal of Consent or Authorization. Company agrees to notify the Business Associate of any changes in or revocations of the consent or authorization provided to Company by individuals pursuant to 45 C.F.R. §164.506 or §164.508, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

3.3 Restrictions on Use or Disclosure. Company agrees to notify Business Associate of any restrictions or limitations on the use or disclosure of PHI to the extent such restrictions may affect the Business Associate's use or disclosure of PHI.

3.4 Permissible Use by Company. Company agrees not to request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy/Security Standards if done by Company.

SECTION 4 – CHAIN OF TRUST AND TRADING PARTNERS

4.1 Chain of Trust. This Addendum is intended to create a chain of trust agreement within the meaning of the Security Standards with respect to electronically exchanged data whereby all parties to this Addendum agree to protect the integrity and confidentiality of all PHI exchanged. The sender and receiver depend upon each other to maintain the integrity and confidentiality of the transmitted information.

4.2 Compliance with Standard Transactions. If Business Associate conducts Standard Transactions for on behalf of Company, Business Associate will comply, and will require any subcontractor or business associate involved with the conduct of such Standards Transactions to comply, with each applicable requirement of 45 C.F.R. §162.

SECTION 5 – SECURITY OF ELECTRONIC PHI

5.1 Security. Business Associate will (i) implement, maintain and use appropriate and effective administrative, technical and physical safeguards to reasonably preserve the confidentiality, integrity, and availability of electronic PHI as required by the HIPAA Security Standards; (ii) ensure that any Business Associate, including a subcontractor, to whom Business Associate provides electronic PHI agrees to implement reasonable and appropriate safeguards to protect the electronic PHI; and (iii) report to Company any security incident immediately upon becoming aware of such incident.

5.2 Direct Access to Company Systems. In advance of being granted access to Company systems, Business Associate acknowledges and agrees, and will require any subcontractor or Business Associate involved in the direct access to acknowledge and agree, that (i) all information contained in the Company information system is considered to be confidential data, including, but not limited to, patient, financial, proprietary, trade secret, intellectual property, and other business data; (ii) access and access methods to Company information shall be held in confidence with agreement to exercise all necessary control over such information so as to avoid the possibility of disclosure or other misuses; (iii) information obtained through direct access will not be shared with any other individual or organization unless specifically authorized by this Addendum or in a separate writing by Company; (iv) information will be used for the functions of the job for which access is authorized; (v) access to Company information shall be strictly controlled to only those individuals with job function need-to-know basis; (vi) codes or passwords used to access Company systems shall not be disclosed to individuals not included in this Addendum; and (vii) immediate notification will be provided to Company of any compromise of a code or password or use by an unauthorized person.

5.3 Compliance with Federal Rules and Regulations: Business Associate acknowledges its obligation and agrees to comply with all applicable provisions of the HITECH Act and the HIPAA Security Rule §164.98 (Administrative Safeguards), §164.312 (Technical Safeguards), and §164.316 (Policies and Procedures). If Business Associate accesses, receives, maintains, retains, modifies, records, destroys, or otherwise creates, holds, uses, or discloses Unsecured Protected Health Information, Business Associate agrees to notify Company immediately when it discovers a Breach of such information. In any event written notice shall be given no later than sixty (60) days. Business Associate agrees that it shall notify the Company Privacy Officer of such Breach at (405) 280-5711 or by email to

compliance@globalhealth.com and follow up with notice in writing to include, to the extent possible, the following elements: (1) identification of the individuals whose information was Breached; (2) a brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known; (3) a description of the types of Unsecured Protected Health Information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (4) any steps individuals should take to protect themselves from potential harm resulting from the Breach; (5) a brief description of what Business Associate is doing or plans to do to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches; and (6) contact procedures for Company or its Members to ask questions or learn additional information, which should include a toll-free telephone number, an e-mail address, Website, or postal address. Business Associate agrees to fully cooperate with Company to provide notice to affected individuals as required by law.

SECTION 6 – AVAILABILITY, AUDITS AND INSPECTIONS

6.1 Availability of PHI. Business Associate agrees that it will, upon prior written notice, make available during normal business hours at Business Associate's offices, all records, books, agreements and policies and procedures relating to the use and/or disclosure of PHI to Company to enable Company to determine the Business Associate's compliance with the terms of this Addendum and applicable laws and regulations governing PHI.

6.2 Access to DHHS. Business Associate shall make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by one party on behalf of the other available to the Secretary of the Department of Health and Human Services ("DHHS"), governmental officers and agencies for purposes of determining compliance with the Privacy/Security Standards and this Addendum.

6.3 Assistance with Investigations, Audits, and Monitoring Responsibilities. Business Associate specifically agrees to assist Company and/or participate in any investigation and/or audit conducted by any government enforcement agency, outside legal counsel, or the Company's Compliance/Privacy Officer or representative by (i) permitting inspection of records and documents maintained by Business Associate in connection with services provided pursuant to this Addendum; and/or (ii) complying with any other reasonable requests of Company in connection with an investigation, audit and/or monitoring responsibility of Company imposed by the Privacy/Security Standards.

SECTION 7 – TERM/TERMINATION

7.1 Term and Termination. This Addendum is on the Effective Date and shall remain effective for the entire term of the Underlying Agreement, or until terminated as set forth herein.

7.2 Termination Without Cause. Company shall have the right to terminate this Addendum for any reason with sixty (60) days written notice to Business Associate.

7.3 Termination for Breach. Company may immediately terminate this Addendum and the Underlying Agreement without penalty if Company makes the determination that the Business Associate has breached a material term of this Addendum. Alternatively, Company may choose to (i) provide the Business Associate with thirty (30) days written notice of the existence of the alleged material breach and (ii) afford the Business Associate an opportunity to cure said alleged material breach upon mutually

agreeable terms. Failure to cure in the manner set forth in this section is grounds for immediate termination of this Addendum and the Underlying Agreement.

7.4 Return/Destruction of PHI. Business Associate agrees that, upon termination, cancellation, expiration or other conclusion of the Underlying Agreement or this Addendum, for whatever reason, it will, if feasible, return or destroy all PHI received from, or created or received by it on behalf of Company which Business Associate maintains in any form, and retain no copies of such information. Business Associate will complete such return or destruction as promptly as possible, but no later than thirty (30) days after the effective date of the termination, cancellation, expiration or conclusion of the Underlying Agreement or this Addendum, at which time an authorized representative of Business Associate shall certify in writing to Company that all PHI has been returned or disposed of as provided above and that Business Associate no longer retains any such PHI in any form.

7.5 No Feasible Return/Destruction of PHI. To the extent such return or destruction of PHI is not feasible, Business Associate shall identify any PHI that Business Associate created for or received from Company that cannot feasibly be returned to Company or destroyed. Business Associate will extend the precautions of this Addendum to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information not feasible. Business Associate will certify in writing to Company the identification of any PHI for which return or destruction is not feasible and, for that PHI, will certify that it will only use or disclose such PHI for those purposes that make the return or destruction not feasible. Business Associate shall remain bound by the provisions of this Addendum, even after termination of the Underlying Agreement, until such time as all PHI has been returned or otherwise destroyed as provided in Section 7.4.

SECTION 8 – INDEMNIFICATION

8.1 Indemnification. Business Associate shall indemnify and hold Company, any affiliates, officers, directors, employees and Agents, harmless from and against all claims, liabilities, judgments, fines, assessments, penalties, awards or other expenses, of any kind or nature whatsoever, including, without limitation, reasonable attorneys' fees, court or proceeding costs, expert witness fees, and costs of investigation, litigation or dispute resolution, relating to or arising out of any claim, including third-party claims caused by the conduct of Business Associate, its employees, Agents and subcontractors, based on (i) any breach or alleged breach of this Addendum; or (ii) any negligence of wrongful acts or omissions, including the failure to perform its obligations under the Privacy/Security Standards. This indemnification obligation is not subject to any limitation in any other agreement between Business Associate and Company.

SECTION 9 – MISCELLANEOUS

9.1 Construction. This Addendum applies to all past, present and future contracts or relationships between the parties, written or unwritten, formal or informal, in which Company provides PHI to Business Associate. This Addendum shall be construed as broadly as necessary to implement and comply with the Privacy/Security Standards. The parties agree that any ambiguity in this Addendum shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the Privacy/Security Standards.

9.2 Notice. All notices and other communications required or permitted pursuant to this Addendum shall be in writing, addressed to the party at the address set forth at the end of this Addendum,

or to such other address as either party may designate from time to time. All notices and other communications shall be mailed by registered or certified mail, return receipt requested, postage pre-paid, or transmitted by hand delivery or by a nationally recognized overnight courier. All notices shall be effective as of the date of delivery or on the date of receipt, whichever is applicable.

9.3 Modification of Addendum. The parties recognize the this Addendum may need to be modified from time to time to ensure consistency with amendments to and changes in applicable federal and state laws and regulations, including, but not limited to, HIPAA. Upon the effective date of any final regulation or amendment to such applicable state privacy law or regulation, the Addendum and the Underlying Agreement shall be automatically amended such that the obligations they impose on Business Associate remain in compliance with such laws and regulations. Upon request by Company, Business Associate agrees to promptly amend the terms of this Addendum to conform to any applicable change in law or regulation. Business Associate agrees to amend its agreements with its subcontractors and Agents to conform to the terms of this Addendum. Company may terminate this Addendum and the Underlying Agreement upon fifteen (15) days written notice in the event (i) Business Associate does not promptly amend the Addendum when requested by Company pursuant to this section; or (ii) Business Associate does not amend the Addendum sufficient to satisfy the standards and requirements of any applicable state or federal law or regulation regarding the privacy or security of information of Company. Except as otherwise specifically stated herein, this Addendum shall not be waived or altered, in whole or in part, except in writing signed by the parties.

9.4 Transferability. Company has entered into this Addendum in specific reliance on the expertise and qualifications of Business Associate. Consequently, Business Associate's interest under this Addendum may not be transferred or assigned or assumed by any other person, in whole or in part, without the prior written consent of Company.

9.5 Governing Law and Venue. This Addendum shall be governed by, and interpreted in accordance with, the internal laws of the State of Oklahoma, without giving effect to its conflict of laws provisions. Oklahoma County, Oklahoma, shall be the sole and exclusive venue for any arbitration, litigation, special proceeding or other proceeding as between the parties that may be brought under, or arise out of, this Addendum.

9.6 Binding Effect. This Addendum shall be binding upon, and shall ensure to the benefit of, the parties hereto and their respective permitted successors and assigns.

9.7 Execution. This Addendum may be executed in multiple counterparts, each of which shall constitute an original and all of which shall constitute but one Addendum.

9.8 Gender and Number. The use of the masculine, feminine or neuter genders, and the use of the singular and plural, shall not be given an effect of any exclusion or limitation herein. The use of the word "person" or "party" shall mean and include any individual, trust, corporation, partnership, or other entity.

9.9 Priority of Addendum. If any portion of this Addendum is inconsistent with the terms of the Underlying Agreement, the terms of this Addendum shall prevail. Except as set forth above, the remaining non-conflicting provisions of the Underlying Agreement remain in full force and effect.

9.10 No Third-Party Beneficiaries. Nothing express or implied in this Addendum is intended

to confer, nor shall anything herein confer, upon any person other than the Parties and the respective successors and permitted assigns of the Parties, any rights, remedies, obligations or liabilities whatsoever.

9.11 Independent Contractor Status. Both parties expressly acknowledge and agree that Business Associate is at all times acting and performing as an independent contractor. No relationship, other than independent contractor, is or has been created between the parties. Neither party has any right as an agency, employee, joint venture or partner in the business of the other. Neither party shall combine its business operations in any way, but instead, both parties shall maintain their own independent operations as separate and distinct businesses.

SECTION 10 – DEFINITIONS

10.1 Breach. The term ‘‘Breach’’ is the unauthorized acquisition, access, use, or disclosure of Protected Health Information which compromises the security or privacy of the Protected Health Information (“PHI”). An impermissible use or disclosure is presumed to be a Breach unless the Company or Business Associate, as applicable, demonstrates a low probability that the PHI has been compromised, based on a risk assessment that includes at least the following factors: (1) the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; (2) the unauthorized person who used the PHI or to whom the disclosure was made: (3) whether the PHI was actually acquired or viewed; and (4) the extent to which the risk to the PHI has been mitigated.

The following do NOT constitute Breaches:

- Unintentional acquisition, access, or use of PHI by an employee or individual acting under the authority of Company or a Company business associate,
- Inadvertent disclosure of PHI from one person authorized to access PHI at Company or a Company business associate to another person authorized to access PHI at Company or a Company business associate, and
- Unauthorized disclosures in which an unauthorized person to whom PHI is disclosed would not reasonably have been able to retain the information.

10.2 Business Associate. The term “Business Associate” shall mean the Business Associate identified in the first paragraph of this Addendum, along with its affiliates, officers, directors, shareholders, employees, Agents, subcontractors, or persons or entities under Business Associate’s control.

10.3 Company. The term “Company” shall mean GlobalHealth Holdings, LLC and all of its subsidiaries and affiliates**.**

10.4 Designated Record Set. The term “Designated Record Set” shall mean a group of records maintained by or for Company that is (i) the medical records and billing records about Individuals maintained by or for Company; (ii) the enrollment, payment, claims adjudication, and case or medical management, record systems, maintained by or for a health plan; or (iii) used, in whole or in part, by or for Company to make decisions about Individuals. As used herein, the term “Record” means any item, collection, or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for Company.

10.5 Disclose or Disclosure. The terms “disclose” or “disclosure” shall mean the release,

transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

10.6 HIPAA. The term "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, as amended from time to time.

10.7 Individual. The term "Individual" shall have the same meaning as the term "individual" in 45 CFR 164.501 and shall include a person who qualifies as a personal representative under 45 CFR 164.502(g).

10.8 Individually Identifiable Health Information. The term "Individually Identifiable Health Information" shall mean information that is a subset of health information, including demographic information collected from an individual; and (1) is created or received by a healthcare provider, health plan, employer or healthcare clearing house; and (2) relates to the past, present or future physical or mental health or condition of an individual, the provision of healthcare to an individual; or the past, present or future payment for the provision of healthcare to an individual; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

10.9 Material Alteration. The term "Material Alteration" shall mean any addition, deletion or change to the PHI of any subject other than the addition of indexing, coding and other administrative identifiers for the purpose of facilitating the identification or processing of such information.

10.10 Member. The term "Member" shall mean any individual covered under Company's HMO insurance products.

10.11 Privacy/Security Standards. The term "Privacy/Security Standards" shall mean the privacy and security standards implemented pursuant to the HIPAA, as amended from time to time, and any state or federal privacy or security law or regulation

10.12 Protected Health Information or PHI. The term "Protected Health Information" or "PHI" shall mean any individually identifiable health information, transmitted or maintained in any form or medium, concerning any Company member or the patient of any healthcare provider of Company.

10.13 Security Incident. The term "security incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.

10.14 Services. The term "Services" shall mean those services provided by Business Associate to Company.

10.15 Unsecured Protected Health Information. The term "Unsecured Protected Health Information" or "Unsecured PHI" shall mean PHI that is not protected through encryption, destruction, or other method specified by the Secretary of DHHS which would render the PHI unusable, unreadable, or indecipherable to unauthorized persons.

10.16 Use. The term "use" shall mean, with respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains or has possession

of such information.

IN WITNESS WHEREOF, the parties have hereunto set their hands effective the day and year first above written.

PLAN:

GlobalHealth Holdings, LLC.
210 Park Avenue
Suite 2800
Oklahoma City, OK 73102-5621

By: _____
R. Scott Vaughn, President and CEO

BUSINESS ASSOCIATE:

_____
(Printed Name of Business Associate)

By: _____
(Business Associate Signature)

Code of Conduct

Our Commitment

GlobalHealth is committed to doing business in an honest and ethical manner, and in compliance with applicable Federal and State laws, regulations, policies, and contractual requirements. In support of our compliance commitment, GlobalHealth has established a Code of Conduct. The Code of Conduct communicates the basic principles and standards of behavior expected in our work environment and the responsibility we all share for helping GlobalHealth remain in compliance.

This Code of Conduct has been approved by senior management and our governing board and is designed to promote honest, ethical, and lawful conduct by all employees, officers, directors, agents, and first tier, downstream, and related entities ("FDRs"). Your actions have an effect on our reputation and integrity. That is why it is important for you to read this Code of Conduct carefully so that you can understand and abide by its content.

→ All GlobalHealth employees, officers, directors, agents, and FDRs are required to read the Code of Conduct and sign a Compliance Certification form.

Reference policy #GH-CO-002.

Compliance Program

GlobalHealth maintains a comprehensive, effective Compliance Program to ensure compliance with applicable Federal and State laws and regulations, including those pertaining to Federal Health Care Programs (e.g., Medicare, Medicaid, Federal Employees Health Benefits Program (FEHBP), etc.). Our Compliance Program includes, at a minimum, the required elements in the Office of the Inspector General ("OIG") model compliance program guidance, U.S. Federal Sentencing Guidelines, and compliance program requirements from The Centers for Medicare and Medicaid Services ("CMS"). This includes: (1) designated Chief Compliance Officer; (2) Code of Conduct; (3) written policies and procedures; (4) auditing and monitoring; (5) education and training; (6) methods for reporting compliance concerns, including a toll-free anonymous hotline; (7) periodic risk assessments; and (8) disciplinary, corrective, and/or remedial action when compliance concerns are identified.

→ All GlobalHealth employees, officers, directors, agents, and FDRs must complete appropriate compliance training upon employment, contract execution, or appointment, and annually thereafter.

Reference policy #GH-CO-001. Also see 42 CFR §§422.503(b)(4)(vi) and 423.504(b)(4)(vi); CMS Publication #100-16, Chapter 21; and CMS Publication #100-18, Chapter 9.

Reporting Compliance Violations

GlobalHealth employees, agents, officers, directors, and FDRs have an obligation to report compliance violations or concerns, including violations of GlobalHealth policy or the Code of Conduct. Reports may be made directly to the Chief Compliance Officer ("CCO") or Compliance Department or through a 24-hour toll-free anonymous reporting hotline. All reports concerning a potential compliance violation are investigated by the CCO and held in the strictest confidence possible depending on the nature of the report.

GlobalHealth has a strict non-retaliation policy. Anyone who in good faith reports a violation, or assists in an investigation of a possible violation, will not be intimidated or retaliated against.

→ Methods for contacting Compliance

CCO Direct Phone:	(405) 280-5711
Toll-free:	1-877-280-5852 (anonymous 24-hour hotline)
Email:	compliance@globalhealth.com
FAX:	(405) 280-5894
Address:	ATTN: Compliance Officer GlobalHealth 210 Park Avenue Suite 2800 Oklahoma City, OK 73102-5621

Reference policy #GH-CO-003.

Fraud, Waste & Abuse ("FWA") Program

An important part of the Compliance Program is to ensure adequate methods for prevention, detection, and deterrence of Fraud, Waste, and Abuse (FWA).

Fraud is knowingly and willfully executing, or attempting to execute, a scheme or artifice to defraud any health care benefit program (such as Medicare) or to obtain by means of false or fraudulent pretenses, representations, or promises, a payment or benefit from the health care benefit program.

Waste is the overutilization of services, misuse of resources, or other practices that directly or indirectly result in unnecessary costs to the Medicare Program.

Abuse includes actions that may, directly or indirectly, result in unnecessary costs to the Medicare Program, improper payments, payment for services that fail to meet professionally recognized standards of care, or services that are medically unnecessary.

Examples of FWA include (but are not limited to):

1. Falsifying documents or submitting fraudulent documentation/reports to the government in order to obtain financial or other benefit.
2. Upcoding or billing for items/services that are not documented in the medical record or were not provided.
3. Forged prescriptions.
4. Member sharing their ID card with someone else.
5. Routine ordering of medically unnecessary services.
6. Duplicate charging / billing.
7. Receiving an overpayment from Medicare and keeping it.

GlobalHealth employees, agents, officers, directors, and FDRs are expected to participate in the prevention, detection and reporting of FWA. This includes participation in required FWA training. Do not worry about deciding whether something is fraud, waste, or abuse. If you have reason to suspect possible FWA, you have a duty to notify the CCO or FWA manager.

Reference policy #GH-CO-013.

The Federal False Claims Act

The Federal False Claims Act ("FCA"), 31 U.S.C. §§3729-3733 and 3801-3812, and similar state laws, prohibit the knowing presentation of false or fraudulent claims to the Federal or State governments. Fraudulent and abusive activities may include knowingly (1) billing for services not provided; (2) including incorrect codes or charges on bills to receive higher reimbursement; (3) forging, altering or destroying documents to secure payment; or (4) making or using, or causing to be made or used, a false record or statement in order to receive payment or benefit.

The FCA may be violated even without specific intent to defraud the government. A person or entity acts "knowingly" if he/she/it has actual knowledge that the act is fraudulent, or acts in deliberate ignorance or reckless disregard of the truth. In other words, the standard is, "knew or should have known." Examples: (1) you suspect that a coworker is committing fraud but you choose to ignore it; (2) you do something that you believe may be incorrect based on guidance or policy; and (3) you are not sure whether it is correct, and you fail to review the policy or procedure or ask for guidance.

Violations of the FCA include fines of up to three (3) times the dollar amount claimed (referred to as "treble damages") and civil monetary penalties ("CMP") from $5,500 to $21,000 for each false claim. A violation of the FCA may also result in forfeiture of participation in Federal health care programs (i.e., no longer being able to participate in the Medicare Program).

Individuals who believe that Federal health care program billing requirements have been violated may pursue alternative administrative or legal remedies under the FCA or State law and cannot be retaliated against for reporting such a violation. Individuals with knowledge of false claim billing may also file a lawsuit on behalf of the United States government and receive a percentage of any recoveries.

→ If you believe there is a potential FCA situation, report it to Compliance.

Anti-Kickback Statute

The Anti-Kickback Statute ("AKS"), 42 U.S.C. §1320a-7b(b), provides penalties against anyone who knowingly and willfully solicits, receives, offers, or pays remuneration, in cash or in kind, to induce or in return for (1) referring an individual to a person or an entity for the furnishing or arranging for the furnishing, of any item or service payable under the Federal health care programs or (2) purchasing, leasing, ordering, or arranging for or recommending the purchasing, leasing, or ordering of goods, facilities, services, or item payable under the Federal health care programs.

Individuals and entities that engage in unlawful referral or kickback schemes may be subject to criminal penalties, civil monetary penalties, or exclusion from participation in Federal health care programs.

→ GlobalHealth is committed to compliance with the AKS. Anyone who is aware of a potential AKS violation should report it to the CCO.

Reference policy #GH-CO-008.

Conflicts of Interest

A conflict of interest occurs when a relationship or private interest influences or impairs, or may give the appearance of impairing, your ability to make objective and fair decisions in the performance of your job or is contrary to GlobalHealth's business interests. Employees, and those acting on behalf of GlobalHealth, should avoid situations that might force choosing between personal interests and the interests of GlobalHealth.

It is not possible to describe or anticipate all circumstances and situations that involve a conflict of interest, but below are a few examples that might be a potential conflict.

- Direct or indirect financial interest in, or in a financial, consulting, managerial or employment relationship with, a company that is a competitor, customer, or a supplier of goods and services to GlobalHealth.
- Solicitation or acceptance, directly or indirectly, of gifts, payments, or other benefits from customers, suppliers, or those doing business or seeking to do business with GlobalHealth.
- Receiving personal honoraria for services performed that are closely related to the individual's job duties with GlobalHealth.
- Employment in a second job or having a relationship with a competitor or other entity where the nature of that job or relationship places the individual in a conflict with GlobalHealth's interests.
- Using information, property, or one's position with GlobalHealth for personal gain.
- Acquiring, directly or indirectly, real property, leaseholds, or other property or rights in which GlobalHealth has, or the individual has reason to believe at the time of acquisition, that GlobalHealth is likely to have an interest.
- Serving on a board of directors or similar body of a for-profit company or government agency.

You are free to engage in outside activities that do not interfere with the performance of your responsibilities to GlobalHealth or that are in conflict with GlobalHealth interests. Although GlobalHealth encourages professional

activities and community involvement, care should be taken not to compromise duties owed to GlobalHealth.

→ If you have questions concerning a possible conflict or are aware of a conflict of interest situation involving yourself or someone else, or need to disclose a conflict of interest, please report this to the Compliance Officer.

Reference policy #GH-CO-016.

Use of Company Assets and Property

Assets or property belonging to GlobalHealth may only be used for legitimate, authorized business purposes. You may not (1) take, use, or knowingly misappropriate Company assets or property for personal use or gain, or for use by another, or for an improper, unethical, or illegal purpose; (2) remove, dispose of, or destroy anything of value belonging to GlobalHealth without GlobalHealth's consent; (3) take for yourself personally any opportunities discovered through the use of GlobalHealth's property, information, or position. Additionally, you should not engage in the unauthorized use, copying, distribution, or alteration of computer software.

Competition and Antitrust

GlobalHealth complies with applicable antitrust and similar laws that regulate competition. Examples of conduct prohibited by antitrust laws include: (1) agreements to fix prices; (2) bid rigging; (3) collusion with competitors; (4) boycotts; (5) certain exclusive dealing; (6) price discrimination agreements; (7) unfair trade practices including bribery, misappropriation of trade secrets, deception, intimidation, and (8) similar unfair practices. These behaviors and situations must be avoided.

Privacy and Security of Information

GlobalHealth complies with Federal and State laws and regulations concerning the privacy and security of Protected Health Information ("PHI"), including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Health Information Technology for Economic and Clinical Health ("HITECH") Act. Member/Patient health information is confidential and should not be released without proper authorization.

PHI includes any information that can identify an individual (e.g., name, address, phone, account number, email address, date of birth, SSN, etc.) and has to do with the individual's past, present, or future health status. GlobalHealth must take reasonable precautions to safeguard PHI. This includes, but is not limited to, the following:

(1) Read and follow GlobalHealth policies pertaining to privacy and security of PHI including the Notice of Privacy Practices ("NPP").
(2) Do not discuss PHI with affiliates or coworkers unless necessary for business purposes.
(3) Do not discuss PHI with your family and friends or other outside party. Do not post confidential company information or PHI on social media.
(4) Shred all documents containing PHI. Do not put confidential information in a regular trash can – only use bins that are labeled as confidential shred bins.
(5) Log off computer screens when not in use.

(6) Always use an approved, completed FAX cover sheet when faxing confidential information.

(7) Do not email PHI without proper authorization. If you are sending a confidential email, make sure it is properly encrypted and includes an approved privacy disclaimer.

(8) Change your computer password often. Do not share your password or post it where others can see. Make sure your password is secure: an ideal password contains at least eight (8) characters with a combination of numbers, alpha, symbols, and upper and lower cases, and is not a word found in the dictionary.

(9) Ensure that any electronic devices used outside our facilities, whether company owned or personally owned, have the proper safeguards including encryption. This includes laptops, tablets, USB (thumb/flash) drives and cellphones/smartphones.

→ If you have any question concerning a privacy or confidentiality matter or believe a HIPAA privacy violation may have occurred, contact the GlobalHealth Privacy and Information Security Officer as soon as possible at (405) 280-5524 or email privacy@globalhealth.com. Or, call the toll-free hotline at 1-877-280-5852 and leave a message.

Reference policies #GH-HI-001 – 010.

Network / Computer Use

Any individual who accesses or uses the GlobalHealth computer network system must follow system use agreement requirements and policies. This includes safeguarding electronic information and mobile devices and taking all reasonable precautions to protect confidential information stored on computers. PHI must be secured in accordance with requirements established by HIPAA, HITECH, and other applicable federal and state regulations. Breaches of unsecured PHI may result in serious fines and penalties. Additionally, there are notification requirements for breaches of unsecured PHI, including reporting such breaches to the affected parties, the government, and the media. GlobalHealth issued computers, equipment, and wireless, etc. should not be used to visit inappropriate websites.

→ If you are aware of an improper disclosure or breach of PHI, or if you have lost or misplaced a mobile device containing PHI, notify the GlobalHealth Privacy and Information Security Officer (call 405-280-5524 or email privacy@globalhealth.com) and the Help Desk (helpdesk@globalhealth.com) immediately.

Reference policies #GH-HI-001 – 010.

Sales and Marketing

GlobalHealth's marketing and advertising must be truthful and not misleading. Claims about GlobalHealth products or services must be supported by evidence to substantiate the claim. Further, GlobalHealth must comply with specific marketing rules that pertain to Medicare Advantage plans. Anyone responsible for sales or marketing of Medicare products must complete approved specialized training, testing, and compliance attestation each year.

→ If you are aware of questionable sales or marketing practices, notify the Compliance department.

Reference policy #GH-CO-006. Also see CMS Publication #100-16 – Medicare Managed Care Manual, Chapter 3.

Workplace Behavior

General

GlobalHealth is committed to a work environment that respects the rights, dignity, and cultural differences of its work force. GlobalHealth expects that all employees and associates will conduct themselves in a professional manner both in the work place and at any time or location while representing GlobalHealth. Employees should refer to the Human Resources (HR) Tab on the GlobalHealth intranet site for updated HR policies.

Harassment

GlobalHealth does not tolerate harassment in the work place. Harassment occurs when one's conduct creates an intimidating, offensive, or hostile environment that interferes with work performance. Harassment may include, but is not limited to, the following: inappropriate verbal conduct, such as racial, ethnic or religious epithets or sexual innuendos; display of inappropriate materials; use of inappropriate gestures; transmitting sexually suggestive, derogatory, or offensive materials via GlobalHealth computers or accessing such information while at work; assault; unwanted physical contact, coerced sexual conduct, touching, patting, or pinching; and threats or demands to submit to sexual requests. Harassment, or any other form of physical, mental, or verbal abuse or disruptive behavior, is inappropriate and will not be tolerated. Anyone who believes he or she has been unlawfully harassed should promptly report this to his or her supervisor, HR director or the Compliance Officer.

Reference policy #GH-HR-205.

Weapons

Weapons are prohibited in the GlobalHealth workplace, whether legally permitted or not.

Drugs/Alcohol

GlobalHealth is committed to providing a drug-free work environment. All job applicants must pass a drug screening test prior to employment. The illegal possession, distribution, or use of any controlled substances on company premises or at company functions is strictly prohibited. Reporting to work under the influence of any illegal drug or alcohol is also prohibited. Employees may be asked to undergo drug testing in certain situations as defined by written policy and State law.

Reference policy #GH-HR-309.

Smoking/Tobacco

GlobalHealth maintains a tobacco-free, smoke-free environment; this includes a restriction on the use of electronic cigarettes (e.g., vaping) on any GlobalHealth leased or owned property.

Reference policy #GH-HR-307.

Work Attire

Employees and agents are expected to display a professional appearance at work and while representing GlobalHealth. This includes maintaining proper grooming and business attire.

Reference policy #GH-HR-308.

Solicitation

To promote an atmosphere conducive to productivity and free of undue pressure, GlobalHealth does not permit anyone to sell or solicit other employees to purchase goods or contribute money to non-Company approved fundraisers in work areas or during work time.

Travel Safety

Everyone is expected to obey all traffic laws when operating a vehicle for company business purposes. This includes not texting or emailing when driving.

Accounting and Recordkeeping

All GlobalHealth records must be prepared accurately, reliably, honestly, and in accordance with established finance/accounting or other written procedures. Entries of cost, financial or other business information are made only to the regularly maintained books and records. GlobalHealth has a system of administrative and accounting controls to (1) safeguard its assets; (2) check the accuracy and reliability of its accounting data; (3) promote operational efficiency; and (4) comply with laws and regulations.

All records must be stored in a secure location for the period of time required by law or by policy, whichever is longer – typically ten (10) years. Records should be organized in a manner that permits prompt retrieval. Records that are no longer needed, either in paper or electronic form, must be properly disposed of, or purged, in accordance with applicable record retention policies. A record should never be destroyed in anticipation of, or in response to, a request for those documents by any government agency, court, or litigation hold.

→ Know and follow the record retention policies that apply to your area. If you are not sure, ask your supervisor or contact the Compliance Department.

Reference policy #GH-CO-011.

Hiring or Contracting with Ineligible or Excluded Individuals or Entities

GlobalHealth will not credential, hire or contract with individuals or entities that: (1) have been excluded within the last five years from any Federal health care program (e.g., Medicare, Medicaid, CHAMPUS); (2) are owned or controlled by individuals who have been convicted, sanctioned, and/or excluded from a Federal program; (3) have been convicted of a criminal offense that would trigger exclusion from a Federal program; or (4) are proposed for sanction by a program. All individuals employed by or contracted with GlobalHealth must notify GlobalHealth of the occurrence of any of the above listed actions.

GlobalHealth conducts pre-employment screening of all new employees against the Office of the Inspector General ("OIG") list of excluded individuals and entities at http://exclusions.oig.hhs.gov and https://www.sam.gov. Such screenings are also conducted on network providers, contractors, and vendors. Follow-up screening is performed monthly. Non-contracted providers are screened prior to any claims payment. FDRs are expected to screen their employees, contractors and subcontractors in accordance with GlobalHealth policy.

Reference policy #GH-CO-004.

Claims Processing and Determinations

GlobalHealth complies with applicable Federal and State laws and regulations pertaining to payment of claims for services, including those from The Centers for Medicare & Medicaid Services ("CMS"), as applicable. GlobalHealth takes reasonable measures to ensure that claim determinations are made accurately and timely. Individuals who work in claims areas are expected to understand and comply with applicable Federal health care program requirements, contractual agreements, and GlobalHealth policies related to claims adjudication and payment.

Standard clinical admissions criteria that include medical necessity guidelines are used to determine whether or not reimbursement may be made for inpatient care. Authorization determinations are made based on established criteria and are made without discrimination, prejudice, or bias.

→ Seek guidance from management if a policy is unclear or a unique situation arises where you are uncertain how to proceed.

Reference policy #GH-CO-007.

Interactions with Regulatory Agencies and Government Officials

GlobalHealth is honest in its dealings with regulatory agencies and government officials, and complies with applicable reporting and disclosure requirements. GlobalHealth employees, directors, officers, affiliates, representatives, agents, and FDRs must not attempt to influence, bribe, or have dealings with government officials that are, or would give the appearance of being, illegal or unethical.

→ Consult the CCO for any questions concerning communication with or reporting to a regulatory agency or government official.

Reference policy #GH-CO-018.

Non-Discrimination and Affirmative Action

GlobalHealth complies with federal and state employment laws and does not discriminate in its hiring practices with regard to age, race, color, gender, religion, national origin, ethnicity, disability, gender identity, gender assignment, sexual orientation, or veteran status. GlobalHealth is an Equal Opportunity Employer and affirmatively seeks to recruit, employ, and advance qualified protected veterans and qualified individuals with disabilities.

→ If you are a supervisor, or in a position to make hiring decisions, make sure you understand GlobalHealth's employment-related policies and relevant laws. If you don't know, contact the CCO or HR.

Reference policy #GH-CO-019.

Disciplinary Action

One of the elements of an effective compliance program is consistent enforcement of compliance through corrective, remedial, and/or disciplinary action. In accordance with our Compliance Program, GlobalHealth takes appropriate and timely corrective action when non-compliance situations are discovered.

Further, GlobalHealth has a written disciplinary action policy that provides guidance for consistent handling of employee matters (e.g., Code of Conduct violations, policy violations, and other non-compliance situations, misconduct, etc.).

Reference policy #GH-CO-012.

Policies

GlobalHealth employees, agents, directors, officers, and FDRs are expected to adhere to GlobalHealth's policies and are responsible for knowing where and how to access those policies. Policies are maintained on the GlobalHealth intranet site http://polaris/sites/1greatteam/policies/default.aspx. Compliance policies are available for outside entities (agents, FDRs, providers, etc.) through the internet applicable tab.

It is not possible to anticipate every decision or action that you might face or encounter. If you have any doubt about the right ethical or legal choice to make, review GlobalHealth policies for guidance, or seek direction from the responsible manager or the Compliance Department.

Below is a list of Compliance policies as of the print date of this Code of Conduct. Note: This list is not inclusive of all GlobalHealth policies. Please review policies periodically, at least annually.

Compliance Policies	Description
- GH-CO-001	Compliance Program
- GH-CO-002	Code of Conduct
- GH-CO-003	Reporting Compliance Concerns (including the toll-free hotline)
- GH-CO-004	OIG Exclusion Screening
- GH-CO-005	Non-Retaliation
- GH-CO-006	Medicare Marketing
- GH-CO-007	Claims Payment
- GH-CO-008	Anti-Kickback Statute
- GH-CO-009	Appeals & Grievances
- GH-CO-010	FDR Oversight
- GH-CO-011	Record Retention
- GH-CO-012	Disciplinary Action
- GH-CO-013	Fraud, Waste, and Abuse (FWA)
- GH-CO-014	Advance Directives
- GH-CO-015	Compliance Audit Plan
- GH-CO-016	Conflict of Interest
- GH-CO-017	Social Media Use

- GH-CO-018 Dealing with Regulatory Agency or Government Officials
- GH-CO-019 Non-Discrimination and Affirmative Action
- GH-CO-020 Contract Management
- GH-CO-021 Policy Approval Process
- GH-CO-022 Risk Adjustment Program

HIPAA Policies	Description
- GH-HI-001	Privacy Policy
- GH-HI-002	Breach Notification
- GH-HI-003	Release of PHI
- GH-HI-004	Email
- GH-HI-005	FAX
- GH-HI-006	Information Security
- GH-HI-007	Remote Access
- GH-HI-008	Mobile Computing Devices
- GH-HI-009	Amendment of PHI
- GH-HI-010	Destruction of Confidential Materials

HR Polices	Description
- GH-HR-205	Anti-Harassment
- GH-HR-307	Tobacco and Smoke-Free Policy
- GH-HR-309	Substance Abuse

Finance Policies	Description
- GH-FIN-007	Business Expense Reimbursement

Compliance Certification

I have read the GlobalHealth Code of Conduct and will abide by its contents.* I understand that it is my responsibility to bring known or potential violations of the Compliance Program, Code of Conduct, applicable laws or regulations, or GlobalHealth policy to the attention of the Compliance Department. I understand that I will not be retaliated against or punished for my good faith report or inquiry.

I know how and where to access GlobalHealth's compliance polices and any other policies relevant to my job. I also understand that it is my responsibility to periodically review the GlobalHealth Code of Conduct and policies and to seek guidance from management or the GlobalHealth Chief Compliance Officer if I have any questions.

Print Name_____ Title _____

Signature_____ Date _____

Your Department or Company Name (if FDR):_____

*Please state below any known or potential conflict of interest or other situation that might prevent you from fully complying with the Code of Conduct, Compliance Program, or GlobalHealth policies.

_____
_____
_____
_____
_____
_____

Sign and return this form to Human Resources or your designated contact.

The Code of Conduct supports GlobalHealth's Mission, Vision, and Values.

Mission

We are driven by our passion to deliver the best healthcare coverage in the industry. We are committed to continuous innovation and comprehensive member engagement to earn the satisfaction and confidence of those we serve.

Vision

- We aspire to earn and retain provider confidence and trust in us.
- We aspire to be the clear choice for health insurance.
- We aspire to offer our affordable healthcare products nationwide.
- We aspire to be the employer of choice in our industry, attracting and retaining a highly talented workforce.
- We aspire to continuously innovate.
- We aspire to achieve member confidence in all we do.

Values

- We believe managing and navigating healthcare should be easier.
- We support a culture of empowering, valuing and encouraging our employees.
- We believe our model of change and positive disruption will continue to support our mission.
- We are committed to active listening and respecting differing opinions to gain meaningful solutions and positive results.
- We are committed to ongoing, effective and impactful communications within the organization.
- We believe in developing and maintaining valued relationships with our partners.

GlobalHealth
701 NE 10th ST | Ste. 300 | Oklahoma City, OK| 73104-5403

GlobalHealth Holdings, LLC
Contracted Medicare Advantage Product
FMO Agent Appointment Packet Checklist

Name _____ National Producer Number _____

The following is the return list:

- ☐ Packet Checklist page
- ☐ Completed Broker/Producer/Agent Appointment Application Questionnaire
- ☐ Completed Consumer Authorization and Release, signature on page 1 and page 2
- ☐ Signed Individual Agent Attestation
- ☐ Signed Business Associate Addendum, page 10
- ☐ Signed Code of Conduct Compliance Certification, page 12
- ☐ Hierarchy Form with name and phone number
- ☐ Copy of E&O Insurance Certificate, Expiration Date:_____
- ☐ Copy of your valid Oklahoma Insurance License, Expiration Date:_____
- ☐ Copy of AHIP Certificate

Please return the listed documents with all required signatures to:

Email: nancy.adams@globalhealth.com
Fax: (918) 878-7373

Hierarchy Form

	Please Print	Contact Information	For Office Use Only
Producer's Name			
Managing General Agent's Name			
Company Name			
GlobalHealth Representative Name			