JIVA PROVIDER PORTAL SERVICE AGREEMENT

This Agreement sets forth the terms, obligations and conditions between **Alliance Health** (hereinafter referred to as "Alliance"), with a business address at **5200 W. Paramount Parkway, Suite 200, Morrisville, NC 27560**, and _____ with a business address at _____ (hereinafter referred to as "Provider"), with regard to the JIVA Provider Portal access contemplated herein.

RECITALS

WHEREAS, this Agreement is ancillary to the Network Participating Provider Agreement ("Contract") executed between the Parties, and the terms of the Contract are fully incorporated herein by reference;

WHEREAS, Alliance utilizes and engages in the electronic transmission of data through use of Secured Technology Platforms that include the ZeOmega JIVA Platform. Alliance utilizes JIVA as our Population Health Platform to view and retrieve the records of members for the purposes of treatment, payment, or certain health care operations and for other permissible purposes pursuant to the Health Insurance Portability and Accountability Act of 1996, and the rules and regulations promulgated thereunder, as may be amended from time to time (collectively, "HIPAA"), and further subject to the American Recovery and Reinvestment Act of 2009 ("ARRA"), including its provisions commonly known as the Health Information Technology for Economic and Clinical Health ("HITECH") Act, and rules and regulations promulgated thereunder, as may be amended from time to time. The Provider Portal allows access to sensitive information, which is confidential by law, regulation, or policy, or which is proprietary in nature (collectively, the "Data"). These Provider Portals are accessed by login credentials including a unique User Identifications ("User ID") and password;

WHEREAS, Alliance believes that proper use of the portal would be beneficial and desires to permit Provider access to the JIVA Provider Portal ("Portal") subject to the restrictions and other requirements set forth in this Agreement; and

WHEREAS, the Provider desires to enter into an Agreement with Alliance to obtain access to Data within the JIVA Provider Portal utilized by Alliance for treatment, payment, or health care operations purposes that are related to Provider's obligations under the Contract and that another source is not capable of meeting those needs;

THEREFORE, Alliance and the Provider (hereinafter individually referred to as a "Party" and collectively as the "Parties") hereby agree to the following terms, obligations and conditions:

Effective Date and Term. This Agreement shall become effective upon complete execution by all Parties. The Term of this Agreement for Provider access to the JIVA Provider Portal through Alliance shall begin on **May 1, 2024, and continue unless terminated.**

Limitations on Access. Provider hereby agrees that access under this Agreement is limited, conditional, non-assignable, and non-transferrable, pursuant to the provisions and specifications identified in this Agreement (hereinafter collectively referred to as "Access"). The Provider agrees to ensure that its users understand the limited and restricted nature of the access being provided and the related responsibilities.

Authorized Users. Only the Provider and designated users who are directly employed by Provider are permitted to access to the JIVA Provider Portal. Provider understands and warrants that such access and use shall be limited to that achieved through unique access IDs provided to each Authorized User granted access by Alliance, and that each Authorized User shall be prohibited from sharing their login information or using another Authorized User's access ID to access the Provider Portal. This agreement does not permit subcontractors to Provider, such as billing companies and data analytics consultants, to be users; Provider's payors are also not permitted to be users under this agreement.

Each provider will be required to complete and sign the Alliance Health Portal Access Request form (Attachment A) and submit it with this Agreement. Each individual user will be required to review the Alliance Portal Confidentiality Agreement (Attachment B).

Appropriate Access to and Use of Information. Provider and its users will only access those records for members with whom they have a relationship or when the need to establish a relationship has been identified; only access the minimum information needed to accomplish a legitimate treatment, payment, or health care operations purpose; and only use and share the information from JIVA Provider Portal in an appropriate manner and for proper purposes. In no event are Provider or its users to use the access or the information for personal or unapproved uses or objectives. User access is subject to audit and inappropriate access may result in corrective action up to termination of access to the JIVA Provider Portal. Inappropriate access would constitute a breach on the Provider's behalf. Provider shall work with Alliance's Privacy Officer in following the breach notification investigation and process.

Supervision and Training of Users. Provider is responsible for the supervision, acts and omissions of itself and its users; this includes verifying that access to the JIVA Provider Portal, specific members, and the use and disclosure of the information is proper and appropriate.

Each Authorized User will be required to complete, in a form and in a manner to be determined by Alliance, reasonable training regarding the user requirements of the Portal, such training to be coordinated through the Site Administrator. Access to the JIVA Provider Portal shall be on a need-to-know basis and dependent upon the Provider's job duties.

Responsibility for Information. Once the Provider and its users are in possession of information from the JIVA Provider Portal, they are responsible for the protection of that information. Provider is liable for any associated use, disclosure, transmission, access, incidents, or breach of such information and agrees to indemnify and hold Alliance harmless from any related claims, penalties, damages, cost, expenses, and liabilities related to Provider's and users' associated acts or omissions. Provider and its designated employees shall be vigilant in identifying any errors encountered while accessing or using the JIVA Provider Portal and will report any such encounters to medicalrecords@alliancehealthplan.org. Such encounters may include, but is not limited to, documentation under the incorrect member record or a document uploaded to the incorrect member record.

Security Safeguards. Provider and its users will safeguard the JIVA Provider Portal and information accessed, including:

- Protect access credentials (User ID, password, etc.) at all times and not share them with anyone, including co-workers, supervisors, contractors, or agents.
- Provider nor its personnel will download, modify, delete, or attempt to download, modify, or delete any such records or other information or content located therein.
- Secure workstations and any other devices used to access the JIVA Provider Portal, such as by logging out or locking screens.
- Immediately contact Alliance at PrivacySecurity@alliancehealthplan.org and cooperate with all investigations and remediation efforts if Provider's or users' access or credentials are compromised, lost, or stolen at any time or something unusual or suspicious is observed while accessing the JIVA Provider Portal.

Provider is responsible for securing all necessary hardware, software, and interoperability requirements to effect access at its own cost and expense. Alliance is not responsible for the procurement, installation, integration, or maintenance of any Components, and Alliance makes no representations or warranties regarding the Components whatsoever.

Provider acknowledges that Alliance does not guarantee constant or consistent availability of the JIVA Provider Portal, and that the portal may be periodically unavailable due to technical issues, security concerns, or hardware and software maintenance and upgrades.

If Alliance has any good faith concerns that Provider's systems or connections pose a threat to the security and privacy of the information in the JIVA Provider Portal, Alliance may immediately terminate the connections and access.

Mandatory User Access Review and Notifications. Alliance will submit to Provider a current and updated list of approved users no less than every six (6) months. Provider will immediately notify Alliance at PrivacySecurity@alliancehealthplan.org when any or all granted access is no longer necessary, such as if a user changes roles or departs Provider's organization. Alliance may require Provider to attest that it and its designated users continue to have a legitimate need for access to the JIVA Provider Portal and Provider will comply with such requests in a timely manner.

Reporting of Unauthorized Use or Disclosure of PHI. Within five (5) business days of becoming aware of an unauthorized access, use or disclosure of PHI arising from use of the System by any third party or by Provider, its officers, directors, employees, contractors, agents or by a third party to which Provider disclosed PHI from the Portal (a "Disclosure"), Provider shall report any such Disclosure to Alliance. Such notice shall be made by contacting Alliance at PrivacySecurity@alliancehealthplan.org and by letter sent via a nationally recognized overnight carrier to the following:

Privacy Officer
Alliance Health
5200 W. Paramount Parkway
Suite 200
Morrisville, NC 27560

Provider's Privacy/Security Officer shall investigate and mitigate, any known or suspected breach of this Agreement by Providers designated employees, owners, and directors. Further, Privacy/Security Officer shall promptly notify Alliance of: (i) any actual or suspected Breach as defined by 45 CFR 164.402, or any actual or suspected security incident including any attempted or actual exploit or vulnerability such as phishing, malware, distributed denial of service attack, or other event that may or could adversely impact the security, integrity or availability of the PHI, of which Officer becomes aware,

or any other confidentiality, privacy or security claim or complaint, arising out of, or relating to or otherwise connected with the Alliance Member records accessed or used by Provider; (ii) any subpoena, demand, request, or other inquiry from any governmental or regulatory entity made to the Provider, arising out of, in connection with or otherwise relating to this Agreement; (iii) any suspension or separation from provider's employment of any employee granted access to the Portal; (iv) any change in the employee's job duties that alter or terminate such access to the Portal or member records.

Health Insurance Portability & Accountability Act of 1996 ("HIPAA"). Provider explicitly acknowledges and understands that it is required to comply with any and all laws relating to privacy and/or security of protected health information ("PHI") or other healthcare, public assistance or social services information, including but not limited to HIPAA and its implementing regulations, 45 CFR Parts 160, 162 & 164, as further expanded by the Health Information Technology for Economic and Clinical Health Act (HITECH Act), which was adopted as part of the American Recovery and Reinvestment Act of 2009, commonly known as "ARRA" (Public Law 111-5) and any subsequent modifications thereof, the Substance Abuse Confidentiality regulations set forth in 42 CFR Part 2, N.C.G.S. § 122C-51, *et seq.*, N.C.G.S. § 108A-80,10A NCAC Subchapter 26B, and DMH/DD/SAS Confidentiality Rules published as APSM 45-1 (effective January 2005).

Confidentiality of Other Information (Non-PHI). "Confidential Information" shall mean any materials, written information, and data marked "Confidential" by Alliance or non-written information and data disclosed by Alliance that is identified at the time of access by/disclosure to the Provider as confidential but shall not include PHI or healthcare, public assistance or social services information protected by HIPAA or other confidentiality laws. Provider shall take affirmative measures to protect Confidential Information, and, to the extent permitted by law, to maintain the Confidential Information in strict confidence for a period as specified by the applicable state and federal record retention schedules for each Enrollee served, either in original paper copy or an electronic/digital copy. The term "Confidential Information," as used herein, does not include any information which: (a) meets the definition of a public record under the NC Public Records Law; (b) is in the public domain; (c) has been made public other than by acts by the Provider in violation of this Agreement; (d) that is independently known, obtained or discovered by the Provider; (e) that is hereafter supplied to the Provider by a third party without restriction; or (f) becomes available to Provider on a non-confidential basis.

Data Ownership. Provider acknowledges and agrees that Alliance owns all rights, interests, and title in and to all data acquired, accessed, or viewed through the Portal, and that such rights, interests, and title shall remain vested in Alliance at all times. Provider shall not compile and/or distribute such data or any analyses to third parties utilizing any data received from, or created or received on behalf of, Alliance without express written permission from Alliance or the applicable patient. This extends to Protected Health Information (PHI) and Personally Identifiable Information (PII). Notwithstanding, certain records available for Provider's access through the Portal may be copied and used by Provider only to the extent permitted by applicable laws and regulations.

Intellectual Property Rights. ZeOmega owns and retains exclusive ownership of all right, title and interest in and to (i) the Software and any copies thereof including all modifications, improvements, Updates, and Upgrades; (ii) the Documentation and any copies thereof; (iii) any Feedback; and (iv) all Intellectual Property Rights embodied within and the Derivative Works thereof in the foregoing (i)-(iii). Accordingly, Provider agrees that ZeOmega exclusively owns any and all Deliverables (excluding Alliance Intellectual Property therein, if any), software, documentation, Feedback, templates, Object Code, Source Code, middleware, APIs, interfaces, connectors, software layers, shims, work flows, engines, flow charts, documentation, information, reports, results, findings, ideas and any and all works and other materials developed hereunder by ZeOmega, and the Intellectual Property Rights therein

and Derivative Works thereof (collectively, the "ZeOmega Intellectual Property") and that all title, right and interest thereto shall remain solely with ZeOmega.

Restrictions. Provider may not: (a) reproduce, modify, translate, prepare Derivative Works or, disassemble, de-compile, reverse engineer, or otherwise attempt to determine the Source Code or protocols from the Object Code of the Software or knowingly permit or encourage any third party to do so, (b) resell, sub-license or distribute the Software either individually or as part of another software, (c) use the Software in any manner to provide service bureau, time-sharing or other computer to third parties other than for the use of the Authorized Users, (d) use the Software in any manner to assist or take part in the development, marketing, or sale of a product potentially competitive with the Software, (d) use the Software, or allow the transfer, transmission, export, or re-export of the Software or portion thereof in violation of any export control laws or regulations administered by any government agency or (e) remove, obscure, or alter any copyright notice, trademarks, logos and trade names, or other proprietary rights notices affixed to, or contained within the Software.

Investigation/Sanctions/Audits. Alliance reserves the right to monitor, review and investigate reported and identified failures to comply with this Agreement and impose reasonable nonmonetary appropriate sanctions. Sanctions may include, but are not limited to, the termination of this Agreement or termination of an Authorized Users' access. Alliance reserves the right to report unprofessional conduct to appropriate licensing or other regulatory authorities. Provider agrees to reasonably cooperate with Alliance to adequately investigate complaints received involving the Provider's employees or agents. Further, Provider agrees to reasonably cooperate with Alliance in the event of a regulatory agency investigation regarding Alliance and Provider's use of the Portal.

Provider understands and agrees that compliance with this Agreement may be audited by Alliance at any time. If requested, Provider agrees to cooperate promptly and fully, and to cause its designated employees, owners, and directors to so cooperate in any such audit, including without limitation, prompt provision of a written explanation of the purpose(s) of any Member record access or use or disclosure, as well as any subsequent access, use or disclosures of same.

Cooperation with Oversight Activities. Provider agrees to cooperate with Alliance in its oversight activities and shall take such corrective action as is necessary to comply with State and Federal law and any Accreditation Standards. Provider further agrees to provide timely, accurate, and appropriate data and information to enable Alliance to fulfill applicable accrediting organizations' and Federal and State regulatory filing requirements, provided the disclosure of such information is consistent with applicable State and Federal laws regarding confidentiality.

Termination. The rights and remedies of Alliance provided in this section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Agreement.

Alliance may, by written notice to the Provider, terminate the Agreement immediately, if, in the judgment of Alliance:

(a) Provider has materially breached this Agreement; or
(b) Provider is in violation of any law, rule or regulation; or
(c) Provider fails to timely submit required reports, records or documentation as required under this Agreement;
(d) Provider is no longer eligible to provide the Services required under the Provider Network Contract; or
(e) Provider fails to cure any breach of protected health information.

Unless prohibited by law or other contractual obligation, Provider understands, acknowledges, and

agrees that Alliance may terminate this Agreement without liability at any time, without cause, within the sole discretion of Alliance upon thirty (30) days' written notice to Provider.

Compliance with Laws. Both Parties agree to implement this Agreement in strict compliance with all applicable federal, state, and local laws, rules and regulations.

Assignment. The Parties may not assign or subcontract duties, rights, or interests under this Agreement unless the other Party provides written consent. If Alliance approves further delegation of functions, those functions shall be subject to the terms of this Agreement and in accordance with the accreditation standards of Alliance's National Accrediting Body.

Insurance. Provider shall maintain, at its sole cost and expense, commercial general liability insurance on an occurrence basis in the minimum amount of $1,000,000, from companies that are authorized to provide such coverage. Such insurance shall also provide Cyber Liability and/or Error's & Omission's coverage sufficient to cover the full replacement value of invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion, and network security of Alliance property that will be in the care, custody, or control of Provider.

Upon execution of this Agreement, Provider shall furnish to Alliance a Certificate of Insurance reflecting the minimum limits stated above. The Provider shall provide for thirty (30) days' advance written notice in the event of a decrease, termination, or cancellation of coverage. Providing and maintaining adequate minimum insurance coverage is a material obligation of the Provider. All such insurance shall meet all laws, rules, regulations, and requirements of the State of North Carolina. The limits of coverage under each insurance policy maintained by the Provider shall not be interpreted as limiting the Provider's liability and obligations under the Agreement.

Force Majeure. Alliance shall not be liable for any delay or failure to perform its obligations due to circumstances beyond Alliance's control, such circumstances to include without limitation natural disasters, terrorism, labor disputes, war, declaration of governments, transportation delays, computer and/or network failures, acts of civil or military authorities, interruptions in third-party telecommunications or Internet equipment or service, and misuse of Software by Provider.

Indemnification. To the fullest extent permitted by laws and regulations, Provider shall indemnify and hold harmless Alliance and its officials, agents, and employees from and against all claims, damages, losses, and expenses, direct, indirect, or consequential (including but not limited to attorneys' fees and costs related to court action or mediation) arising out of or resulting from Provider's Portal access under this agreement or the actions of Provider under this Agreement or under contracts entered into by the Provider in connection with this Agreement. This indemnification shall survive the termination of this Agreement. Notwithstanding the foregoing, nothing contained in this Agreement shall be deemed to constitute a waiver of the sovereign immunity of Alliance as a local political subdivision of the State of North Carolina, which immunity is hereby reserved to Alliance.

Notice. All notices (including material change in Provider's ability to perform), reports, records, or other communications which are required or permitted to be given to the Parties under the terms of this Agreement shall be sufficient in all respects if given in writing and delivered in person, by confirmed facsimile transmission, by overnight courier, or by registered or certified mail, postage prepaid, return receipt requested, to the receiving party at the following address:

If to Alliance: Alliance Health
Attention: Office of Legal and Public Affairs
5200 W. Paramount Parkway, Suite 200
Morrisville, NC 27560

If to Provider: _____
Attention: _____
_____
_____

Governing Law and Forum. This Agreement shall be governed by and in accordance with the laws of the State of North Carolina. All legal actions brought by either Party hereunder relating in any way to this Agreement shall be brought in the General Court of Justice in Wake County, North Carolina.

Entire Agreement. This Agreement, including Attachment A, constitutes the entire understanding between the Provider and Alliance with respect to the subject matter hereof, shall supersede all prior understandings and Agreements relating to the subject matter hereof, and may not be amended except by a written Agreement signed by the Provider and an authorized representative of Alliance.

IN WITNESS WHEREOF, each Party has caused this agreement to be executed in multiple copies, each of which shall be deemed an original, as the act of said Party. Each individual signing below certifies that it has been granted the authority to bind that Party to the terms of this Agreement and any attachments thereto.

Provider	**Alliance Health**
By: _____	By: _____
Print Name: _____	Print Name: _____
Title: _____	Title: _____
Date Signed: _____	Date Signed: _____

ATTACHMENT A
PORTAL ACCESS REQUEST

This form is used to request a login and password for access to applications in the Alliance Health Provider Portal for an employee to use in performance of their job duties as described below. The form is also used to revoke an employee's access who no longer requires access. A member of the Provider's Senior Management is required to complete, sign and submit the form or appoint a provider representative who can request access for and deactivations of the applications. Once the form is complete, please email to privacysecurity@alliancehealthplan.org. Complete additional sheets as needed.

Provider and User Contact Information:	Tax ID:
Provider Name:	Provider Main Phone Number:
Provider Representative Requesting Access:	Title of Provider Representative:
	Direct Telephone Number:
	Work Email Address:
Provider Privacy and/or Security Officer:	Direct Telephone Number:
	Work Email Address:

Application Portal Access:

☐ JIVA Population Health Management Utilization Management (SAR Submission)

Business Need for Access:

☐ **ADD** OKTA/ JIVA **access for staff submitting** SARs

By signing below, you agree to provide the Confidentiality Agreement (Attachment B) to staff for whom you are requesting access to the Portals.

_____	_____	_____
Provider Signature	Provider Print Name	Date

ATTACHMENT A
PORTAL ACCESS REQUEST

Employee Name:	Title/Primary Role:
Work Email Address:	Telephone Number:
◯Activate ◯Deactivate	
Employee Name:	Title/Primary Role:
Work Email Address:	Telephone Number:
◯Activate ◯Deactivate	
Employee Name:	Title/Primary Role:
Work Email Address:	Telephone Number:
◯Activate ◯Deactivate	
Employee Name:	Title/Primary Role:
Work Email Address:	Telephone Number:
◯Activate ◯Deactivate	
Employee Name:	Title/Primary Role:
Work Email Address:	Telephone Number:
◯Activate ◯Deactivate	
Employee Name:	Title/Primary Role:
Work Email Address:	Telephone Number:
◯Activate ◯Deactivate	
Employee Name:	Title/Primary Role:
Work Email Address:	Telephone Number:
◯Activate ◯Deactivate	
Employee Name:	Title/Primary Role:
Work Email Address:	Telephone Number:
◯Activate ◯Deactivate	

ATTACHMENT B
PORTAL CONFIDENTIALITY AGREEMENT

By using the Alliance Health Provider Portal, I agree to protect the confidentiality, privacy and security of patient, member, business and other sensitive electronic or proprietary information (collectively, "Confidential Information") of Alliance Health from any source and in any form (e.g., verbal, paper, electronic, etc.). I understand that I have an obligation to protect the Confidential Information that I may create, access, use or disclose as part of my job duties including, but not limited to, information regarding the following:

- MEMBERS (such as patient/member records, utilization management, and billing information)
- THIRD PARTIES (such as computer programs, technology)
- OPERATIONS, PERFORMANCE IMPROVEMENT, QUALITY ASSURANCE (such as utilization, data reports, quality improvement)

1. I will protect members' Confidential Information, following all federal and state regulations, statutes, my employer's policies and procedures, and the Provider Contract.
2. I will not post, discuss, or otherwise share any Confidential Information, including patient/member pictures or videos, financial or personal information, on any social media sites such as Facebook, Instagram, or Twitter.
3. I will complete all required privacy and security training.
4. I will only access information that I need to perform my job responsibilities or services at my employer while operating within the Alliance Health Provider Portal and its associated applications.
5. I will not access, show, tell, use, disclose, release, e-mail, copy, give, sell, review, change or dispose of Confidential Information unless required in performance of my job responsibilities. I will follow my employer's policies regarding destruction of Confidential Information (such as shredding confidential papers using confidential lock bins or deleting electronic files from devices), and I will only access or use the minimum necessary information needed to complete the required task.
6. I will not disclose or take with me any Confidential Information when my employment with the Provider ends, whether voluntary or involuntary.
7. I will not use another person's login credentials (user ID or password) to access any system, I will not share my user ID or password, and I will not record my password where someone may find and use it.
8. I will notify Alliance Health's Privacy Officer at privacysecurity@alliancehealthplan.org and change my password immediately if I think someone knows or has used my password.
9. I will tell my supervisor and Alliance Health's Privacy Officer if I am aware of any possible breaches of my username or password.
10. I will report suspected breaches of confidentiality to my supervisor and Alliance Health's Privacy Officer at privacysecurity@alliancehealthplan.org.
11. I will log off the computer when I leave my work area or when the computer will be unattended.
12. I understand that I am responsible for ensuring the privacy and security of Confidential Information at any location (e.g., home, office, etc.). I will position screens to minimize unauthorized viewing of protected health information.
13. I will not store Confidential Information on systems outside of Alliance Health and/or my employer's office systems including on personal computers/devices.
14. I will immediately report any lost or stolen device, personal or otherwise, that was used to access Alliance Health resources according to my employer's procedures.
15. I will not maintain or send Confidential Information to any **unencrypted** mobile or portable storage device.
16. I understand that my access to Confidential Information may be audited at any time.

ATTACHMENT B
PORTAL CONFIDENTIALITY AGREEMENT

I understand that Alliance Health may remove or limit my access to the Alliance Portals and applications at any time.

I understand that my failure to comply with this Agreement may result in the termination of my access rights to the Alliance Portals and applications.

Examples of Breaches of Confidentiality (What you should NOT do)
These are examples only. They do not include all possible breaches of confidentiality.

Accessing information that you do not need to know to perform your job responsibility or services:
- Unauthorized reading of patient/member account information.
- Unauthorized reading of a patient's/member's chart.
- Accessing information on family, friends, or co- workers (being nosey).

Sharing, copying, or changing information without proper authorization:
- Discussing Confidential Information in a public area such as a waiting room, elevator, or hallway.
- Posting a picture of a patient/member on a social media site.
- Commenting on patient/member on a social media site.

Sharing your User ID and password:
- Telling someone your password so that he or she can log into computer system(s) to do their work or yours.
- Giving someone the access codes for employee files or patient/member accounts.
- Leaving a secured application unattended while signed on.
- Being away from your computer while you are logged into the computer.
- Allowing someone to access confidential information using your username and password.