MONUMENT HEALTH, INC.
OUTSIDE PARTY CONNECTION AGREEMENT

This Outside Party Connection Agreement (the "Agreement") is between Monument Health, a South Dakota non-profit corporation ("MH"), and _____ ("Company") (together, the "Parties"). The Purpose of this Agreement is to ensure that appropriate administrative and technical safeguards are in place to protect confidential patient and business data, prior to the establishment of a secure method of connectivity to MH's computer network ("Network Connection") for Company and to provide guidelines for Company's use of MH's computer network and the computing resources associated with the Network Connection.

This Agreement consists of this main document and the following attachments:

Attachment 1: Outside Party Connection Agreement – Terms and Conditions
Attachment 2: Outside Party Connection Request – Information Requirements Document
Attachment 3: Outside Party Network Connections, (current version available from PolicyStat)
Attachment 4: Business Associate Agreement (current version from MH Materials Management department)

This Agreement will become effective on the date set forth in Attachment 1.

This Agreement is the complete agreement between the Parties regarding the subject matter of this Agreement and replaces any prior oral or written communications between the Parties. There are no conditions, understandings, agreements, representations, or warranties, expressed or implied, which are not specified herein. This Agreement may only be modified by a written document executed by the Parties hereto. Any disputes arising out of or in connection with this Agreement shall be governed by South Dakota law.

The Parties have executed this Agreement on the dates indicated below.

_____ ("Company")	**Monument Health Inc. and its Affiliates.**
_____	_____
Authorized Signature	Authorized Signature
_____	_____
Name	Name (Printed)
_____	_____
Date	Date

ATTACHMENT 1

OUTSIDE PARTY CONNECTION AGREEMENT
TERMS AND CONDITIONS

1. Right to Use Network Connection

   Company may use the Network Connection only for business purposes as authorized by MH. Company's request for set-up of a Network Connection shall be made by using the *Outside Party Connection Request - Information Requirements Document* (Attachment 2 to the Agreement).

2. MH-Owned Equipment

   Under the terms of a separate contract between MH and Company, MH may loan or lease to Company certain equipment and/or software ("MH-Owned Equipment") for use on Company's premises.

3. Network Security

   3.1. Company is responsible for ensuring that its employees are not security risks to MH's computer network. Upon MH's request, Company will provide MH with any and all information reasonably necessary for MH to evaluate security issues relating to any Company employee's access to the Network Connection or any MH-Owned Equipment.

   3.2. Company shall assume sole responsibility for protection of their private network(s), which may be interconnected with the MH computer network via the Network Connection.

   3.3. Company shall take all necessary measures to ensure that their private networks are secure, including the following:

      3.3.1. Company agrees that it will implement virus protection and firewall protection if Company has any connection(s) to or with the Internet or Internet enabled email.

      3.3.2. Company agrees that wireless network implementations will utilize industry accepted security protocols.

   3.4. Company agrees to abide by all MH policies related to computing or Information Technology. Company understands that its violation of any such policies may result in MH's immediate termination of this Agreement.

   3.5. If Company does not access the Network Connection for a period of ninety (90) days, MH may suspend the Network Connection. In such event, Company should contact MH's Information Technology Help Desk (605.755.8131) to lift the suspension.

4. Password Use and Maintenance

   4.1. Company understands and agrees that Company employees must be individually authorized by MH and must receive unique user ID and passwords before accessing the Network Connection. The Parties shall work together to compose, maintain, and update a list of mutually agreeable Authorized Company Employees. This list will be kept within MH's Information Technology department. Once a Company employee is authorized, MH will grant the Authorized Company Employee (Employee) a unique username and password to access the Network Connection and specific software applications, as authorized.

4.2. Any distribution of Network Connection passwords by Company must be via a method pre-approved by MH.

4.2.1. MH's Information Technology Division will issue Employees' initial passwords, delivering them to the user directly or to a designated "Tech Champion" at Company. If a password is delivered to a "Tech Champion," he or she shall verify the identity of the Employee and securely deliver the password to the Employee.

4.2.2. Company shall use methods provided by MH for redelivery of passwords in the event an Employee forgets his or her password.

4.2.3. Once delivered to the Employee, the user account and password may not be shared with any other person. Employees are personally responsible for the use of his or her issued account.

5. Auditing

5.1. Company understands and agrees that MH from time to time will audit Company's use of the Network Connection. Company agrees that it will review MH's audit reports and address any issues identified in those reports within thirty (30) days of receipt of such audits from MH.

5.2. Company shall provide all necessary assistance to MH personnel in the investigation and resolution of any security incidents or issues relating to the Network Connection.

6. Notifications.

6.1. Company promptly shall notify MH in writing when, in Company's opinion, a change to the Network Connection is necessary.

6.2. Company shall notify the Information Technology Help Desk (605.755.8131) when an Employee leaves Company or if his or her position no longer requires access to the Network Connection.

6.3. If any Employee believes their password is compromised (i.e., someone else knows their password) they must immediately notify the Information Technology Help Desk (605.755.8131).

6.4. Company understands that MH regularly schedules computer downtimes to allow MH staff to maintain, update and patch MH computer systems and software. Company use of computer resources will be impacted during these downtimes, and alternate manual processes must be utilized for the flow of information. Routine Monthly Computer Downtimes are scheduled the third (3rd) Sunday of each month, beginning at 9 p.m. (MST). For non-routine downtimes, to the extent possible, MH will provide advanced notice to Company regarding scheduling of downtimes.

7. Privacy & Confidentiality

The Parties acknowledge that by reason of the access granted under this Agreement, Company will have access to certain information and materials concerning MH's technology, products, and protected patient health information that is confidential and of substantial value to that party ("Confidential Information"), which value would be impaired if disclosed to any other person or entity. Company agrees that all Employees will complete and return a signed MH Computer Link Agreement before they will be allowed to access the Network Connection.

8. Payment of Costs

   Unless specified otherwise, each Party will be responsible for all costs incurred by that Party under this Agreement, including, without limitation, costs for phone charges, telecommunications equipment and personnel for maintaining the Network Connection.

9. Disclaimer Of Warranties

   Neither Party makes any warranties, expressed or implied, concerning any subject matter of this Agreement, including, but not limited to, any implied warranties of merchantability and fitness for a particular purpose.

10. Indemnification

    Company agrees to indemnify RCMH for any and all damages, including reasonable attorneys' fees, arising out of or in connection with this Agreement and caused by the acts of Company or any of Company's officers, employees, or agents.

11. HIPAA

    Company is solely responsible for ensuring that its employees and agents are knowledgeable about and comply with the Privacy and Information Security components of the Health Insurance Portability and Accountability Act (HIPAA), with specific emphasis on "minimum necessary access and possible penalties associated with non-compliance.

12. Term, Termination and Survival

    This Agreement will become effective on completion of authorized signatures, and will remain in effect for a term of one (1) year. This Agreement shall automatically renew thereafter for terms of one (1) year each unless either Party, no later than thirty (30) days prior to the expiration of the then current term, provides the other Party with written notice of its intent to terminate the Agreement or desire to renegotiate the terms of the Agreement. Either Party may terminate this Agreement for any reason immediately upon notice to the other Party. Termination of this Agreement will be accompanied by immediate termination of the Network Connection. If this Agreement is terminated by either Party prior to the end of any one (1) year term, the Parties will not enter into another agreement regarding the same subject matter until that one (1) year time period has expired.

13. No Influence on Referrals

    It is not the intent of either Party to this Agreement that any remuneration, benefit or privilege provided for under this Agreement shall influence or in any way be based on the referral or recommended referral by either Party of patients to the other party or its affiliated providers, if any, or the purchasing, leasing, or ordering of any services other than specific services described in this Agreement. Company certifies, with its signature to this agreement that it agrees with, and will abide by, this statement regarding referrals.

14. Excluded Party Provision

    Company certifies that neither it, its shareholders, directors, officers, agents or employees are excluded, debarred, suspended or otherwise ineligible to participate in any federal reimbursement programs, or has been convicted , under federal or state law, of a criminal offense related to (i) the neglect or abuse of a patient, or (ii) the delivery of an item or service, including the performance of management or administrative services related to the delivery of an item or service, under the Medicare or Medicaid programs. Company also agrees that if it becomes ineligible to participate in any of the previously listed programs, it will immediately notify RCMH. This Agreement shall be terminated immediately if Company becomes ineligible under any of these programs.

15. Severability

    If for any reason a court of competent jurisdiction finds any provision or portion of this Agreement to be unenforceable, that provision of the Agreement will be enforced to the maximum extent permissible so as to effect the intent of the Parties, and the remainder of this Agreement will continue in full force and effect.

16. Waiver

    The failure of either Party to enforce any of the provisions of this Agreement will not be construed to be a waiver of the right of such Party thereafter to enforce such provisions.

17. Assignment

    Neither Party may assign this Agreement, in whole or in part, without the other Party's prior written consent. Any attempt to assign this Agreement, without such consent, will be null and of no effect. Subject to the foregoing, this Agreement is for the benefit of and will be binding upon the Parties' respective successors and permitted assigns.

18. Force Majeure

    Neither Party will be liable for any failure to perform its obligations under this Agreement, if such failure results from any act of God or other cause beyond the Party's reasonable control (including, without limitation, any mechanical, electronic or communications failure not caused by that Party).

ATTACHMENT 2

OUTSIDE PARTY CONNECTION REQUEST INFORMATION REQUIREMENTS DOCUMENT

OUTSIDE PARTY CONNECTION REQUEST CONNECTION INFORMATION & CHECKLIST		
In accordance with the Outside Party Network Connections policy, this completed Information Requirements Document must accompany all requests for Outside Party Network Connections. **The MH person or group requesting the Network Connection should ensure that this document is completed <u>and all sections are complete</u> before forwarding the request.**		
MH Contact Information ***(To be completed by MH)***		
Contact Name:		
MH Corporation:		
Department:		
Phone Number:		
Pager Number:		
Email Address:		
Outside Party Contact Information ***(To be completed by Outside Party)***		
Name:		
Company:		
Department:		
Manager's Name:		
Phone Number:		
Pager Number:		
Email Address:		
Physical Location of Outside Party Connection ***(To be completed by Outside Party)***		
Physical address of termination point(s) of the Network Connection		
Main Phone Number:		
Regular Business Hours:		
Contact Information of Initially Authorized Company Employees ***(To be completed by Outside Party)***		
Name:	**Phone Number:**	**Email Address:**
If list of all Employees is not initially available, provide a count of the Employees expected to use the Network Connection. Provide a separate list when defined and provide to the MH Information Technology Help Desk.		
Business Justification/Purpose of Network Connection ***(To be completed by MH)*** (Example: contract coder)		

Application Needs ***(To be completed by MH)***
(List applications that you need access to. Example: Meditech, Athena, 3M 360 Encompass)

Network Connection Needs ***(To be completed by MH)***
(Indicate the type of connection is needed)

☐ Citrix Receiver(receiver.regionalhealth.com)
☐ VDI (Virtual Desktop) (vdi.regionalhealth.com)

These two items require the Security Review of Requesting Company's Network section to be completed

☐ Clientless VPN (access.regionalhealth.com)
☐ VPN site to site

Security Review of Requesting Company's Network ***(To be completed by Outside Party)***

Does the workstation require a username and password?	☐ Username or password required **are not** required ☐ Username and password **are** required
Does this workstation connect wirelessly to a network or connect to a network that has wireless capability?	☐ No Wireless network ☐ Wireless network in place – WEP security protocol is being used. ☐ Wireless network in place – WPA security protocol is being used. ☐ Wireless network in place – WPA2 security protocol is being used.
Does the workstation have anti-malware software installed?	☐ Yes ☐ No
Is there a fire wall in use?	☐ PC Firewall ☐ Router based Firewall ☐ Appliance based Firewall ☐ No Firewall
What is the Operating System version for the workstation(s) that will be connecting to Monument Health's Network?	☐ Windows 10 ☐ Windows 8 ☐ Windows 7 ☐ Window Vista ☐ Windows XP ☐ Other (Mac, Linux, etc…). Please Indicate: _____
Are workstation Operating Systems security patches applied on a regular basis?	☐ Security patches are not applied ☐ Security patches are set to be applied automatically on each PC ☐ Security patches are applied monthly ☐ Security patches are applied at some other interval. Please indicate interval: _____

Additional Notes:

ATTACHMENT 3

OUTSIDE PARTY NETWORK CONNECTIONS (POLICY COC-8217-207)

Current version available from ePolicy on the MH home page, print and attach to this document.

ATTACHMENT 4

BUSINESS ASSOCIATE AGREEMENT

Current version available from the MH Materials Management department. If required, attach to this document.