Contractor Terms of Use Agreement:
Access to MEDNAX Systems

This Terms of Use Agreement (the "Agreement") is entered into as of **___________**, 2020 by and between **____________________________** ("Contractor") and **MEDNAX Services, Inc., and its affiliates** ("Company"), for the purpose of allowing Contractor to access and utilize Company's computing resources. Computing resources include all Company owned, licensed, or managed hardware and software, including email and use of the Company network via a physical, remote or wireless connection, regardless of the ownership of the computer or device connected to the network.

With respect to the use of Company computing resources, Contractor and, if applicable, its employees or agents identified on Exhibit A attached hereto and made a part hereof (collectively, "Contractor"), agree as follows:

1. Company's computing resources and all contents generated by or stored therein, are the sole property of Company.

2. Contractor shall only access and utilize Company computing resources in accordance with those policies and procedures established by Company, including, but not limited to, the use of assigned passwords and other Company security procedures. Further, Contractor shall be bound by its own internal policies and procedures related to computer access and privacy of protected health information. In the event that the Contractor's internal policies differ from those of Company, the stricter of the two policies shall be enforced. Contractor shall not attempt, in any manner, to access any Company computing resources other than by established and approved protocols.

3. Contractor shall use the Company computing resources in a professional, proper and lawful manner at all times and shall not use Company computing resources for personal or other non-related business use.

4. Contractor acknowledges that information transmitted through Company computing resources may contain information that is confidential and proprietary to Company and information that is "protected health information", as defined under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Payment Card Industries Data Security Standard ("PCI"). Contractor shall only use such information for the express purpose of those activities that have been agreed upon between Contractor and Company and in accordance with all applicable laws, including, but not limited to, HIPAA and PCI. Contractor shall not resend, distribute, or otherwise provide access to any information transmitted through the Company computing resources other than as agreed upon between Company and Contractor. Contractor shall use appropriate safeguards to prevent the improper or prohibited or unauthorized use or disclosure of Company's information.

5. Contractor shall notify Company Chief Privacy Officer or Chief Information Security Officer in writing within two (2) business days after knowledge of any actual or suspected breach of security or intrusion of the Company computing resources or any suspected unauthorized use or disclosure of PHI. The notice shall include, to the best extent reasonably possible, the identification of each individual whose PHI has been, or is reasonably believed by the Contractor to have been, accessed, acquired or disclosed during the actual or suspected breach.

6. Company reserves the right to examine the content of any electronic messages sent or stored in the e-mail system in order to protect the integrity and security of its systems, and/or to investigate improper or unauthorized use. Company will inform Contractor as soon as reasonably possible in the event that any improper or unauthorized use by an employee or agent of Contractor is discovered. Improper or unauthorized use may result in immediate termination of the Contractor's rights to access Company computing resources.

7. This Agreement, and Contractor's access to Company computing resources, shall automatically terminate on the date Company or its affiliates no longer provide professional services at Contractor's facility. As to each of Contractor's employees or agents identified on Exhibit A, when any or all such employees or agents are no longer employed by or contracted with Contractor, such access to Company computing resources shall immediately terminate. Contractor shall immediately advise Company of such change in an employee's or agent's status with Contractor. Company reserves the right to suspend Contractor's access to Company computing resources for any reason. Company also reserves the right to terminate Contractor's access to the Company computing resources in the event of Contractor's failure to abide by the terms and conditions of this Agreement.

8. At no time during the Term of this Agreement, or after termination, shall Contractor download, redirect, forward, copy or otherwise retain or collect any information contained within Company computing resources, other than as necessary to perform those services by Contractor on behalf of Company.

9. Contractor will indemnify Company for any property damage, personal injury or any third party claims resulting from the acts or omissions of Contractor or its agents or employees while using the Company computing resources.

10. Contractor agrees to ensure that all systems with remote access to the Company computing resources are located in a secured location, not accessible to unauthorized persons and are user/password protected. Contractor will ensure the use of updated versions of commercially reasonable anti-virus protection on all computers or devices that are used to access the Company computing resources, including any software or applications. Contractor agrees to keep its computers updated with commercially reasonable operating system patches, security software (anti-virus) and to use and maintain firewall protection and other computer security features (such as timed lock out screens and password protection).

11. Company reserves the right to audit, monitor and examine the content of any communications sent or stored in its software, applications or systems in order to protect the integrity and security of its systems, and/or to investigate improper or unauthorized use. Company reserves the right to audit remote access sessions if applicable, for the purpose of monitoring compliance with this Agreement. Company will routinely audit Contractor's access to PHI. In addition, Company may request that Contractor review audit reports and initiate its own investigation into any potential inappropriate access and/or disclosure committed by its employees or agents. Company, in its sole discretion, may take any action deemed necessary against any unauthorized use or access to Company's computing resources, including, but not limited to, termination of Contractor's or Contractor's employees' or agent's access to Company's computing resources or immediate termination of this Agreement.

12. The parties are independent contracting parties and nothing in this Agreement is intended to create a partnership, joint venture, employment or other relationship. Contractor employees are not employees of Company and as such are not entitled to the employment benefits provided by Company to its employees.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed and delivered on their behalf as of the day and year first above written.

COMPANY	**CONTRACTOR**
By ________________________	By: ________________________
Print Name __________________	Print Name __________________

NOTE:
Exhibit A shall be completed for each individual identified that requires access to Company computing resources.

SECTION II. CONFIDENTIALITY AND SECURITY AGREEMENT

As a user of Mednax Services, Inc.'s resources, you may have access to confidential information including patient, financial or business information obtained through your association with Mednax Services, Inc. and its affiliates (collectively, "Mednax"). The purpose of this Agreement is to help you understand your personal obligation regarding confidential information. Signed acknowledgement of this form is required prior to issuance of computer network or application credentials (user ID and password).

Confidential information is valuable and sensitive and is protected by law and by Mednax's policies. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended requires protection of confidential information contained within a healthcare information system. Inappropriate disclosure of patient data may result in termination of your access, as well as the imposition of civil or criminal penalties.

Accordingly, as a condition of and in consideration of my access to confidential information, I acknowledge and agree that:

1. I will not access confidential information for which I have no legitimate need to know and for which I am not an authorized user. This includes accessing my own medical or other confidential information without proper access permission. I will only access the minimum necessary information to satisfy my job role or the need of the request.
2. I will not in any way divulge, copy, release, sell, loan, review, alter, post online, destroy or forward outside of Mednax any confidential information unless expressly permitted by existing policy except as properly approved in writing by an authorized official of Mednax within the scope of my association with Mednax.
3. I will not utilize another user's password in order to access any system nor will I reveal my computer credentials to anyone else for any reason. **I accept personal responsibility and understand that I will be held accountable for all activities occurring under my computer credentials**.
4. If I have knowledge of unauthorized access or disclosure of confidential information I will report it immediately to my supervisor and Mednax's Privacy Officer at 800.243.3839 ext. 5525.
5. I will not seek personal benefit or permit others to benefit personally by any confidential information that I may have access to or that I access as an unauthorized user.
6. I understand that all information on Mednax company resources is the property of Mednax and shall not be used or disclosed inappropriately or for personal gain. I also understand that Mednax reserves the right to inspect or monitor any company owned, leased or controlled computer, computer device, network, computer facility, storage device, voice mail or telephone system at any time for any reason and that Mednax may divulge any information found during such inspections or monitoring to any party it deems appropriate. I understand that I should not consider electronic communications to be either private or secure, nor have an expectation of privacy in anything I create, store, send or receive on the Mednax computer and network.

7. I agree to abide by all Mednax’s rules and regulations as specified in Mednax’s security policies unless specifically defined and approved by a separate contractual agreement.
8. I understand that my duty to maintain confidentiality continues after I no longer have access to Mednax information.

I acknowledge that Mednax has an active on-going program to review records and transactions for inappropriate access and I understand that inappropriate access or disclosure of information can result in termination of my access, as well as the imposition of civil or criminal penalties. My signature below indicates that I have read, accept and agree to abide by the requirements of this agreement.

__________________________________ _______________________

Signature Date

Contractor Action Form

Last Name:	
First Name:	
Social Security Number:	
if no SSN, create unique 4-digit ID:	
Gender:	(Select)
Contractor Type:	(Select)
Job Title:	
Office Location:	(Select)
Practice Based - Location / Location Code:	
Division:	(Select)
Region:	(Select)
Department/Business Unit:	
PAU:	
Supervisor (name):	
Supervisor (title):	
Effective Date:	
Active Through (Date):	
Req Number (if applicable):	

Network Accounts Requested (Yes/No):

Network:	(Select)
E-Mail:	(Select)
Other:	(Select)
If other, please specify:	

Comments:	