MTG RESOURCE ACCESS & USAGE STANDARDS

1. MTG FACILITIES AND OPERATIONS

Provider Member will have access to MTG facilities and operations in order to furnish the Services:

1. Provider Member will be listed as a member of MTG's network of providers with information about Provider Member's qualifications and service offerings.

2. MTG will use commercially reasonable efforts to process and maintain Provider Member's insurance credentialing.

3. Perform billing and collection for the Services furnished, including processing patient and insurer payments for the Services.

4. Provider Member will have access to office space, telehealth platform, and electronic health record resources for use only with patients scheduled and billed by MTG.

5. Provider Member is permitted use of MTG's name, logo, trademarks, service marks, marketing materials, or other proprietary information, subject to MTG's approval. Upon termination of the Agreement, Provider Member shall immediately cease all use of MTG Branding and shall remove any references to MTG from Provider Member's materials, websites, or communications.

6. MTG will pay Provider Members for Services furnished pursuant to the Payment schedule and payment terms, attached hereto and incorporated herein as Appendix A. MTG will supply Provider Member with a yearly statement of earnings, if over $600.00. This statement will be made on Form 1099 Miscellaneous Income and will be delivered electronically or by mail to Provider Member by January 31st for the earnings of the preceding year.

MTG General Operations	
☑	Network Listing: Provider Member will be listed as a member of MTG's network of providers with information about Provider Member's qualifications and service offerings.
☑	Provider Account Manager: Provider Member will have access to an MTG Provider Account Manager for assistance with setting practice goals, building and managing an efficient schedule, and establishing healthy boundaries with clients.
☑	Credentialing & Compliance: MTG will assist with credentialing, re-credentialing, and attestation monitoring, and engage in audits and communications to ensure license and insurance compliance
☑	Intake & Scheduling: Intake scheduling including account registration, collection of insurance and credit card information; client scheduling support including automated rescheduling system
☑	Administrative Support: Professional reception, platform support, maintenance of patient database and medical records
☑	Reporting: Provider Portal, business analytics, and monthly financial period reporting
☑	Office Space: Access to furnished office space based on availability, including the option for reserved part-time use of dedicated office
☑	Workers' Compensation: L&I insurance included (Washington and Nevada providers only)

Updated February 2026

Billing, Insurance & Accounting Operations
☑ Patient insurance benefits verification
☑ Insurance claims submission
☑ Payment processing
☑ Collections and statements
☑ Credit card processing including secure credit card storage and online payment options
☑ Twice monthly provider payments

Technology Operations
☑ AdvancedMD EHR & PM license
☑ Telehealth video conferencing platform
☑ HIPAA-compliant online patient portal
☑ Prescription Bundle (ePrescribe functionality; EPCS subscription, Integrated Prescription Drug Monitoring Program)

2. USE OF THE PREMISES

1. Subject to the Membership Agreement, Provider Member may enter and utilize the authorized MTG locations ("the Premises") during normal business hours for the purposes of providing services as described in the Membership Agreement. Provider Member is authorized to utilize the furniture, associated common areas, features and services. Use of the Premises is non-exclusive, short term, revocable, and limited to use and occupancy of certain office spaces at locations based upon these terms and conditions. Parking access is not included for Provider Members unless authorized for that specific location.

2. Provider Member will receive ten (10) one-hour "credits" per calendar month to use to book office space at authorized MTG premises. Credits may only be used for sessions with patients seen as a part of Provider Member's MTG service package. Use of monthly credits is subject to availability of office space at the time of booking. Unused credits will expire at the end of the calendar month and will not roll over or otherwise accumulate.

3. To make a request for recurring weekly office space, Provider Member can submit an Office Space Request Form. Office space requests must be submitted by the 15th of the month in order to take effect by the 1st of the following month. Office space requests will be fulfilled based on availability of space, and alternative options may be offered if the initial request cannot be met.

4. MTG will deliver the Premises in its present "as is" condition. Provider Member agrees not to make alterations to the Premises without the prior written consent of MTG.

5. Provider Member agrees to be solely responsible for any damage to the Premises and its contents caused by Provider Member or its employees and/or invitees.

6. Provider Member may use its own equipment ("Provider Member's Equipment") at the Premises. Provider Members with recurring, reserved office space may store equipment at the Premises, at designated storage areas. MTG reserves the right to deny storage or use of Provider Member's equipment in the Premises at its sole discretion. Provider Member shall at all times be solely responsible for Provider Member's Equipment, and hereby forever releases MTG from any and all liability or causes of action related to or arising from any damage to or loss of Provider Member's Equipment.

7. Upon request by MTG, any and all property issued to Provider Member by MTG (including, without limitation, identification badges and keys to the Premises) shall be returned to MTG immediately.

8. MTG shall have free access to the Premises at all reasonable times, for the purpose of examining the Premises or making any alterations, repairs or improvements thereto which MTG may deem necessary for the preservation of the Premises; provided, however, MTG shall exercise reasonable efforts to avoid or minimize any interference with Provider Member's business operations.

9. Provider Member shall comply with all federal, state, and local laws, and agrees to abide by all rules, regulations and policies applying to the Premises.

10. MTG and Provider Member utilizing dedicated office space agrees to carry insurance coverage appropriate for their activities. For present purposes, the Parties agree that Provider Member shall carry general liability insurance covering Provide Member's use of the Premises, on an occurrence basis, issued by an insurer authorized to conduct business in the State of Washington. The Parties agree that such coverage shall have minimum limits as required by insurance carrier contracts but no less than $1,000,000 with respect to bodily injury or death to one person, minimum limits of $1,000,000 with respect to any one accident, and minimum limits of $1,000,000 with respect to property damage. In view of the risk that arises or may arise out of the Provider Member's conduct or operations, the Parties agree that such insurance shall name MTG as an additional insured. Provider Member agrees to furnish to MTG a copy of the certificate of

insurance and renewal upon receipt of the same. Provider Members who book office space solely using monthly credits are not required to carry General Liability Insurance, and may in consultation with their insurance provider, carry insurance coverage that they deem appropriate for their business activities and business locations.

11. Provider Member shall be solely responsible for, and agrees to indemnify, defend and hold harmless MTG and its directors, officers, employees, agents, successors and assigns as well as other users of the Premises (the "Indemnified Parties") from and against, any and all damages, expenses, liabilities, demands, losses, claims, actions, judgments and costs of any kind including, without limitation, reasonable attorneys' fees (collectively, "Losses"), which any of the Indemnified Parties may incur that are caused by Provider Member, its agents, contractors, employees, and invitees, or arising from or in any manner related to this Membership Agreement or Provider Member's exercise of the Membership Agreement. The foregoing indemnity shall survive the termination of this Agreement.

12. If the Provider Member does not agree with these terms and conditions, they may choose to provide services remotely via approved HIPAA-compliant telehealth software, as far as is allowable by state and federal law, and insurance carrier contracts.

3. DATA SECURITY PROTOCOLS

1. **Definitions.**

The words and phrases listed below, as used in this Exhibit, shall each have the following definitions:

a. "Authorized User(s)" means an individual or individuals with an authorized business requirement to access Covered Entity Confidential Information.
b. "Hardened Password" means a string of at least eight characters containing at least one alphabetic character, at least one number and at least one special character such as an asterisk, ampersand or exclamation point

c. "Unique User ID" means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase or other mechanism, authenticates a user to an information system.

2. **Data Transport.** When transporting Covered Entity Confidential Information electronically, including via email, the Data will be protected by:

a. Transporting the Data within the Covered Entity's or MTG's internal network, or;
b. Encrypting any Data that will be in transit outside the Covered Entity's or MTG's internal network. This includes transit over the public Internet.

3. **Protection of Data.** MTG and Provider Member agree to store Data on one or more of the following media and protect the Data as described:

a. **Hard Disk Drives.** Data stored on local workstation hard disks. Access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

b. **Network Server Disks**. Data stored on hard disks mounted on network servers and made available through shared folders. Access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

c. **Optical Discs**. (CDs or DVDs) in local workstation optical disc drives. Data provided by Covered Entity on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a Secured Area. When not in use for the contracted purpose, such discs must be locked in a drawer, cabinet or other container to which only Authorized Users have the key, combination or mechanism required to access the contents of the container. Workstations which access Covered Entity Data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

d. **Optical Discs**. (CDs or DVDs) in drives or jukeboxes attached to servers. Data provided by Covered Entity on optical discs which will be attached to network servers and which will not be transported out of a Secured Area. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

e. **Paper Documents.** Any paper records must be protected by storing the records in a Secured Area which is only accessible to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

f. **Remote Access**. Access to and use of the Data will be controlled by MTG or Covered Entity staff who will issue authentication credentials (e.g. a Unique User ID and Hardened Password) to Authorized Users.

g. **Data storage on portable devices or media.**

i. Portable devices include, but are not limited to; smart phones, tablets, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook/netbook computers if those computers may be transported outside of a Secured Area

ii. Portable media includes, but is not limited to; optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape), or flash media (e.g. CompactFlash, SD, MMC).

iii. Covered Entity Data shall not be stored on portable devices or media unless authorized within the Terms and Conditions of the contract with Covered Entity. If so authorized, the Data shall be given the following protections:

i. Encrypt the Data with a key length of at least 128 bits.

ii. Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics.

iii. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.

h. MTG and Provider Member will physically secure portable device(s) and media by:

i. Keeping them in locked storage when not in use

ii. Using check-in/check-out procedures when they are shared, and

iii. Taking frequent inventories.

iv. When being transported outside of a Secured Area, portable devices and media with Covered Entity Confidential Information must be under the physical control of an individual with authorization to access the Data.

4. Notification of Compromise or Potential Compromise.

The compromise or potential compromise of Covered Entity shared Data must be reported to Provider Member within one (1) business day of discovery. MTG must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or any Covered Entity including Provider Member.

5. Data Disposition.

When the contracted work has been completed or when no longer needed, Data shall be returned to Provider Member or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

Data stored on	**Will be destroyed by:**
Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portable hard disks) excluding optical discs	Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or Confidential Information	Recycling through a contracted firm provided the contract with the recycler assures that the confidentiality of Data will be protected.
Paper documents containing Confidential Information requiring special handling (e.g. protected health information)	On-site shredding, pulping, or incineration

Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a coarse abrasive
Magnetic tape	Degaussing, incinerating or crosscut shredding