Eye Management

Provider Newsletter

MMM Of Florida Ophthalmology

2020 Q2

Accurate Provider Data is Vital to Members!

The Centers for Medicare & Medicaid Services (CMS) and National Committee for Quality Assurance (NCQA) require plans to maintain accurate provider directories. Please make sure your provider information is up to date with EMI. If you have any changes to your practice, including but not limited to address, phone number or provider additions/terminations, please notify your EMI Provider Relations Representative.

HEDIS

MMM of Florida, have a commitment to guarantee quality in the services offered to all MMM members. A key part of our monitoring process is the Healthcare Effectiveness Data and Information Set (HEDIS) annual audit. HEDIS 2020 captures care delivered from January 1 to December 31, 2019. MMM has contracted with Advantmed, a medical records-retrieval company, to collect medical records on MMM's behalf. Due to current COVID-19 emergency, Advantmed will work with you to obtain the records through fax, remote electronic medical records (EMR) access (if available) or EMR download. HIPAA permits you to disclose your MMM covered patient's medical information to MMM without authorization from your patient.

Relaxing telehealth regulations does not mean relaxing fraud enforcement

By Patricia Calhoun, Patricia Carreiro | FierceHealthcare

The COVID-19 pandemic rapidly expanded telemedicine use. Telehealth currently addresses everything from routine to pandemic-related care. To facilitate this expansion, federal healthcare programs have loosened, at least temporarily, telehealth restrictions. These eased restrictions, however, create increased opportunities for healthcare fraud and abuse, including Anti-Kickback Statute (AKS) and False Claims Act (FCA) violations.

Recent telehealth regulation changes and telehealth scrutiny

The Department of Health and Human Services (HHS) and the Centers for Medicare & Medicaid Services adjusted their telehealth requirements to expand telehealth's ability to serve patients during the pandemic:

- Patients no longer need to reside in designated rural areas or have preexisting relationships with their providers.
- Providers can use a number of everyday communication technologies to provide telehealth services without being fined by HHS' Office for Civil Rights. Providers are, however, required to make good faith efforts to protect patients' privacy, including, among other things, enabling all available encryption and privacy settings and notifying patients of the increased risk of using such technologies.
- Patients can have their telehealth appointments from the convenience and safety of their homes without traveling to medical facilities.
- More services can now be offered via telehealth, including evaluations to determine continued eligibility for hospice care.
- Telehealth providers can waive patient deductibles and copayments without penalties for offering impermissible kickbacks.

•••••• continued on page 2

•••••• continued from page 1

Relaxing telehealth regulations does not mean relaxing fraud enforcement

- In some circumstances, Medicare and Medicaid no longer require physicians to be licensed in the state in which their patients are located.

Despite these changes, some constants remain, such as the scrutiny telehealth providers face from regulators, particularly for AKS and FCA violations.

In the past year, well before the rise of COVID-19, telehealth providers saw two of the biggest Department of Justice (DOJ) takedowns in history for rampant kickback and fraudulent billing schemes. First, in April 2019, the DOJ charged 24 telemedicine and durable medical equipment company executives and physicians for allegedly paying $1.2 billion in illegal kickbacks and bribes related to prescribing unnecessary back, wrist, shoulder and knee braces.

Second, in September 2019, the DOJ charged 35 individuals in a $2.1 billion fraudulent Medicare billing scheme involving alleged kickbacks to telehealth providers ordering genetic tests. Regulators made clear that COVID-19 will not reduce their focus on prosecuting wrongdoing.

For example, the DOJ recently arrested a Georgia man for his alleged role in a conspiracy involving unnecessary COVID-19 tests. Pandemic or not, the telehealth industry is firmly in the crosshairs of heightened government scrutiny and oversight.

Changed regulations may Increase, rather than decrease, enforcement actions

While easing regulations lead many to assume a decrease in enforcement actions, enforcement actions may increase as regulators respond to new opportunities for fraud. Specifically, telehealth services make it easier for fraudsters to pose as physicians and lure patients into sharing their protected health information or installing malware on their devices.
The relaxed telehealth regulations greatly expand the number of patients for whom fraudulent claims can be submitted. Reduced cybersecurity requirements for telehealth communications increase the risk of hackers intercepting or stealing the protected health information necessary to submit fraudulent claims or commit healthcare identity theft.

Such practices will not go unchecked, and telehealth providers should establish protocols to keep from being unwittingly pulled into the crosshairs.

10 considerations to reduce the risk

- Establish mechanisms to verify patient identity.
- Establish or maintain protocols for informed consent and beneficiary initiation.
- Identify states that have waived in-state licensure requirements for telehealth, and establish protocols for disengaging telehealth with patients where the provider is not licensed in the patient state after the pandemic emergency is lifted.
- Establish practice standards for patient examinations and remote prescribing.
- Document and maintain patient encounter records, including all regularly mandated documentation (such as patient eligibility for hospice care).
- Properly code telehealth services to ensure coverage.
- Review vendor agreements and patient incentives to ensure compliance with the AKS, FCA and Civil Monetary Penalties Law.
- Ensure compliance with state credentialing and scope of practice requirements.
- Establish privacy and security protocols for telehealth offerings and related systems.
- Notify patients of the increased risk of privacy issues when using telehealth services and strongly consider using telehealth vendors willing to execute a HIPAA-compliant business associate agreement.

Verifying member eligibility

Please remember to ask your patients for a copy of their member ID card at each visit and verify eligibility and benefits by contacting MMM of Florida at 888-722-7559 or via their Web Portal https://mmm-fl.innovand.com.

Go Green! We Need Your Emails

In efforts to communicate with our providers in a more expeditious and Earth friendly manner, please send an email with your Group Name and Tax ID to: AugusteM@healthnetworkone.com

Marjorie Auguste

305-614-0100 x4536
800-595-9631 x 4536
fax: 305-614-0171
augustem@healthnetworkone.com

Provider Relations

305-614-0100 option 2
800-595-9631 option 2

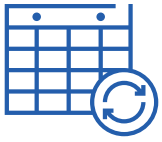
Authorizations

800-595-9631 option 1
Fax: 305-614-0165
Fax: 866-646-1772

Claims

305-614-0133 option 3
954-335-8130 option 3

Annual Diabetic Retinal Exam

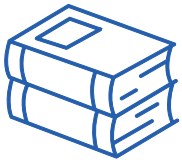


As you know, an annual Diabetic Retinal Exam (DRE) should be part of every diabetic patient's preventive care regimen. In addition, the DRE is a measurement tool used by the National Committee for Quality Assurance (NCQA) to determine if a managed care organization is meeting the health care needs of their member population. Florida Blue is working closely with their Primary Care Physicians and with their members to ensure that they are receiving the preventive services with an eye care professional.

When your patient is in the office we ask that you perform a complete eye exam and document appropriate retinal eye examinations. Please also ensure that you submit a HIPAA 5010 Compliant Claim when billing for these services. It is also extremely important that you document the results of your findings in the patient's chart including No evidence of diabetic retinopathy. We have added this as a separate "diagnosis" (#36) on the Report of Ophthalmic Consultation.

In addition, a report of your findings should be communicated with the member's Primary Care Physician. EMI has a simple template "Report of Ophthalmic Consultation" that you may use. If you need a copy of this form or if you have any questions regarding this information, please contact your Provider Relations Representative, Marjorie Auguste, at (800) 595-9631 x 4536.

Clinical Practice Guidelines



EMI uses Apollo, Milliman Care, or our Health Plan partner Clinical Guidelines (depending on the LOB) for Medical necessity determinations. These guidelines are based on appropriateness and medical necessity standards; each guideline is current and has references from the peer-reviewed medical literature, and other authoritative resources such as CMS Medicare. For any medical necessity Recommendation of Denial, the Medical Director shall make an attempt to contact the requesting provider for peer to peer consultation. The Apollo, Milliman Care, or our Health Plan partner Clinical Guidelines are reviewed and approved by HS1 Medical Advisory committee annually, and are available in both electronic and hard copy format. If a provider would like a copy of a guideline they may contact their assigned Provider Relations Representative and a copy will be provided.

Online Provider Trainings

All providers who currently participate with Eye Management Inc., must complete the Training attestation. The attestation will confirm that your office has received the general trainings for this year. Please click the link https://myemifl.com/trainings/ and fill in the required information in order to complete the attestation for your office. Should you want a copy of the trainings for your office, they can be downloaded from the attestation page.

NOTE: For providers who function under more than one Tax ID; please be sure to complete an attestation for each Tax ID that is contracted with EMI.