



Provider Newsletter

Florida Blue Ophthalmology

2020 Q2

CDC Info Helps You Understand and Treat COVID-19

We're sharing important information from the Centers for Disease Control and Prevention (CDC) to help you understand and treat the disease. Access the most current information on COVID-19 at:

<https://www.cdc.gov/coronavirus/2019-ncov/>

Updates to HEDIS DRE CPT II codes

Diabetic Retinal Exam (DRE):

- Effective October 1, 2019, the CPT II codes 2023F, 2025F and 2033F were added to report the DRE negative result (without evidence of retinopathy).
- Effective October 1, 2019, the CPT II codes 2022F, 2024F and 2026F procedure descriptor were revised to include the DRE positive results (with evidence of retinopathy).
- For measurement year 2020, submit the CPT II code 3072F to report eye exam without evidence of retinopathy performed in 2019 (prior year) by an eye care professional.



Truli for Health (Truli), is a new consumer-centric open-access commercial HMO health plan. The product is scheduled to launch on July 1, 2020 in the following South Florida counties: Broward, Palm Beach, Martin, St. Lucie and Indian River.

Health ID card

Each member has access to a paper ID card and digital card. The nine-digit ID number is listed on the card. Use this number to communicate with us about a member. You can find the following member information on the card:

- Member's ID number
- Member's benefit plan
- Other valuable information, such as where to submit a claim and the group information

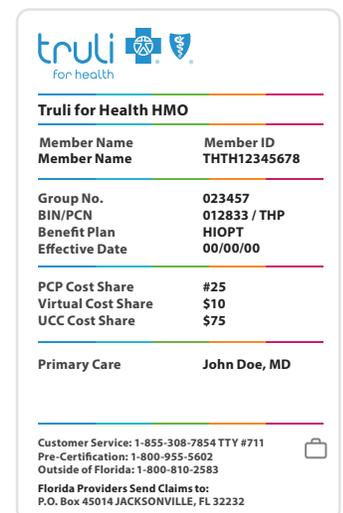
Note: Presenting an ID card in no way creates, nor serves to verify an individual's status or eligibility to receive benefits



Front



Back



Digital ID

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.

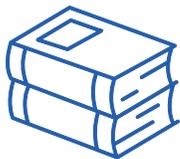
Recent telehealth regulation changes and telehealth scrutiny

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 3

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.

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

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.