Vol. 3,
Issue 3

The Business of Medicine

Leave the business of medicine to us

CODING

How to bill new chronic care management codes

Medicare has created new codes for chronic care management (CCM) in 2015, and the best thing about them is that they're an opportunity to be reimbursed for work your providers already do. In fact, CCM is a service that requires no face-to-face encounter with patients; the only extra task you must perform is to begin documenting and tracking provider work that qualifies as CCM.

CCM is intended to reimburse providers for the work of coordinating and managing patients with chronic conditions, including communication with patients or other treating health care providers. CCM is billed with the new E/M code **99490** (chronic care management services, at least 20 minutes of clinical staff time directed by physician or other qualified health care professional, per calendar month). The average reimbursement for 99490 is approximately $43.

What does CCM involve?

CCM covers all the work your providers and staff routinely perform for patients with chronic illnesses when they aren't in the office. This includes phone calls, refilling prescriptions, and ordering labs or tests. CCM has a minimum time requirement of 20 minutes, so this work only becomes billable if it takes 20 minutes or more. This requirement is made easier by the fact that all work counts toward the 20 minutes, not just work done by physicians or non-physician providers. All clinical staff may contribute toward the 20 minutes so long as it fits the description of CCM for a given patient.

Can your practice provide and be reimbursed for CCM?

Medicare does have several specific rules for CCM in addition to the time requirement. These are outlined below:

(continued on pg. 2)

- **Use of an EHR.** If you don't use an electronic health record (EHR) system at your practice, you'll need to get one up and running before you're eligible to bill for CCM.

- **Patient-centered care plan.** For each patient with multiple chronic conditions, a unique patient-centered care plan must be created. This plan must be accessible 24/7 to all of the practice's clinical staff who will be involved in CCM for that patient.

- **Provider accessibility to patients.** The clinical team involved in CCM for a patient must be accessible to the patient and any other healthcare professionals involved in the patient's care 24/7.

- **Continuity of care.** The practice must be able to provide continuity of care with a designated practitioner or member of the clinical staff whom the patient is able to secure successive routine appointments with. This also requires the practice to provide alternative methods of communication with the patient in addition to the phone, such as secure e-mails.

While CCM is a collaborative effort involving all your clinical staff, the actual claim should be billed under the supervising physician or non-physician practitioner.

How do you identify eligible patients?

Medicare outlines four specific criteria that must be met for a patient to be eligible for CCM:

1. Patient must have multiple chronic conditions (at least two) that your provider is managing.
2. These problems must be chronic, i.e. patients have had them for a minimum of 12 months.
3. These problems place the patient at significant risk of acute exacerbation/decompensation, functional decline, or death.
4. Assuming the above three criteria are met, the patient must agree to participate in CCM. This is because the Medicare annual deductible applies to CCM and 99490 has a co-insurance amount of approximately $8.52 per calendar month billed.

At this time, CMS hasn't published any listing of specific conditions or illnesses that qualify for CCM, and doesn't plan to, so you'll need to rely on the above criteria.

What documentation is necessary for CCM?

CCM has the following documentation requirements, some of which are unique.

- Consent must be obtained from the patient prior to providing CCM. The consent can be obtained on an annual basis and doesn't have to be renewed before each month's CCM claim. The consent form should be similar to the advance beneficiary notice of non-coverage (ABN) form, in that it should explain specifically what CCM covers and how much the patient is responsible for financially.

- The patient must be provided a copy (electronic or otherwise) of their care plan. It's a good idea to have the patient sign an acknowledgement that they have received a copy, so you have proof that this requirement was met.

- The documentation must include a "detailed" accounting of the 20 minutes of CCM time. It should also list the clinical staff involved and what each member contributed to CCM.

- Documentation should include any and all communication regarding the patient's needs and functional deficits to other providers involved in the patient's care.

The code encompasses 30 days of combined services, which for many practices, presents a seemingly overwhelming task of documentation and tracking. Because an EHR is required for CCM, any practice considering CCM should have the systems and tools required for this level of tracking.

First billed, first paid

While the code is most likely to be used by a patient's primary care physician, CMS hasn't explicitly prohibited non-primary care specialties from providing the service. This creates a billing problem, because CCM is a monthly benefit for a patient, and will only be reimbursed by CMS once per month. If multiple providers bill the code on behalf of the patient, the first claim received and processed will be paid.

Example: Mrs. Alexander is 72 and suffers from COPD, DM, HTN, severe spinal stenosis, fibromyalgia, and gout. Her COPD, DM, and HTN are all managed by her primary care physician, Dr. PC, while her pain management provider, Dr. PMP, manages her spinal stenosis, fibromyalgia, and gout. Both physicians provide services that fit the description of CCM. Dr. PMP submits

his claim on Jan. 1, 2015 while Dr. PC submits his claim on Jan. 20, 2015. Because neither the taxonomy nor diagnosis codes on a claim matter for CCM, Dr. PMP's claim would be reimbursed and Dr. PC's claim would be denied.

Unfortunately, this will effectively make CCM a monthly race between providers to get their claim in first.

— Shannon DeConda, CPC, CPC-I, CEMC, CMSCS, CPMA. (sdeconda@drsmgmt.com). The author is founder and president of NAMAS and Director of Coding at DoctorsManagement.

PRACTICE MANAGEMENT

SAGE VIEW

A new insurance strategy for uncertain times

Businesses face increasing uncertainty in today's interconnected global economy. Recent headlines have been dominated by terrorism, data breaches, cybercrimes and employment lawsuits. Unfortunately, most small and medium-sized businesses are underinsured.

In addition to common risks like theft, fire and general liability, there are a host of other, industry-specific risks businesses face that are exacerbated by changes in technology, regulations and the legal system.

Lawsuits are far more common in the current business climate, and lawsuits can come from both outside or inside a company. Businesses face more and more regulations, and it's not uncommon to read a news article about a business crippled or closed down by regulators. Many businesses today also face cyber risks and threats to data security and IT systems. Many of these "new" risks aren't covered by typical third-party insurance policies. These types of coverage often require additional policies that can be very expensive.

So in this climate, what do small and mid-size business owners need most? While different businesses have different needs, almost all would benefit by having a.) More insurance, and b.) More money. But doesn't more insurance mean less money? Aren't they mutually exclusive?

They don't have to be. Here is the most important point. It is possible to significantly increase both insurance and cash reserves simultaneously by owning a captive insurance company. Owning a captive insurance company could be described as formally self-insuring some of the risks faced by a business.

What is informal self-insurance?

Businesses that don't own their own captive insurance company are *informally* self-insuring some of their risks (those not insured by third-party coverage). The result is "taking the risk" and hoping adverse events don't occur. Informally self-insured losses are paid out of operating income, retained earnings, or the owner's savings. There are many reasons that business owners tend to under-insure against the risks they face.

One of the biggest reasons is that insurance premiums paid are a sunk cost. After a year or two or ten with no claims, a business is left at the end of the term with nothing to show for it. It's that simple, there is nothing to show for all those insurance premiums paid, except for peace of mind.

(continued on pg. 5)

MEDICARE RULES

CMS reduces RAC powers to ease provider burden

You can breathe a little easier in 2015 thanks to a slew of new restrictions on the formerly sweeping powers of Medicare's Recovery Audit Contractors (RACs). These private contractors will now have a much shorter look-back period for patient status reviews, less leeway in requesting records from physicians, and must process complex reviews twice as quickly.

CMS is making these changes, among many others, in an effort to address provider concerns about the program, which has been a massive revenue generator for the federal government. RACs recouped $3.75 billion in improper payments from providers in 2013 alone.

Here's a complete list of the changes CMS is making to the RAC program in 2015. These requirements are now part of each RAC's contract going forward:

- **Look-back period reduced.** For patient status reviews, RACs are now limited to a look-back period of six months prior to the date of service, as long as the hospital submits the claim within three months of the date of service. Previously the look-back period was three years. For Part B physicians, the RAC look-back period is unchanged.

- **Reduced ADRs.** RACs will have new limits on the number of additional documentation requests (ADRs) they can send to providers. The new limit will be determined by providers' denial rates; those with lower denial rates will have lower ADR thresholds than those with higher denial rates. Also, providers new to the Medicare program will face fewer ADRs than those who have been participating for many years.

- **More physician reviews.** This isn't necessarily a good change for providers, but RACs will now broaden their reviews of claim and provider types. In 2013 more than 95% of RAC reviews targeted inpatient claims; going forward expect more reviews of Part B claims.

- **Faster resolutions to complex reviews.** RACs conduct automated and complex reviews; the latter involves RAC-employed auditors who examine your claims and documentation to identify any improper payments. RACs must now notify providers of the outcome of any complex review within 30 days, down from 60 days.

- **Standardized RAC websites.** The online web "portals" that RACs offer to allow providers to review claims status will be improved, focusing on making them appear more uniform between the different RACs.

- **Slower RAC payment.** Instead of being paid immediately after recouping monies from providers, RACs will now be paid only after the second level of appeal is exhausted. This change is intended to give RACs more incentive to be accurate in demanding overpayments, CMS said.

- **Reduced overturn rate.** RACs must ensure that fewer than 10% of their first level appeals are overturned. In 2013, approximately 18% of RAC appeals were overturned in favor of providers. RACs that fail to meet this standard will be placed on corrective action plans or possibly be denied the right to conduct certain types of reviews.

Other changes are less definitive, such as CMS's promise to develop a RAC satisfaction survey so you have more ways to share your feedback on the RAC program. You can view the official CMS memo announcing the RAC changes at this link: *www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicare-FFS-Compliance-Programs/Recovery-Audit-Program/Downloads/RAC-Program-Improvements.pdf*.

— Grant Huang, CPC, CPMA (ghuang@drsmgmt.com). The author is Director of Content at DoctorsManagement.

(continued from pg. 3)

Why not over-insure for risks with third party insurance?

Because insurance is a sunk cost, businesses rarely want to be over-insured. So the opposite occurs, and most are under-insured against real risks that could cripple or close their business.

How does owning a captive insurance company help?

The formation of a captive insurance company can help business owners avoid being under-insured without the "sunk cost" of paying insurance premiums to a third party insurer and having nothing to show for it. The business owner or related parties own the captive insurance company. Hence the premiums paid to insure against risks are not "sunk costs." They are insurance reserves and profits owned by the captive owner.

Furthermore, by choosing to formally insure risks through a captive, business owners benefit from insurance law and taxation. Premiums paid by the business to the captive are a business expense, reducing taxable income. Small captive insurance companies are taxed on their underwriting profits at a tax rate of 0%. Small captive insurance companies are defined as receiving $1.2 million or less in annual premiums. Large captive insurance companies (i.e. those receiving annual premiums greater than $1.2 million) also receive favorable tax treatment. Large insurers calculate potential future losses and set aside loss reserves. As such, they pay taxes on underwriting profit only. Loss reserves are not taxed. Both small and large insurance companies are able to invest and grow large pools of assets.

What is a captive insurance company?

A captive is a unique insurance company. It includes its own corporation, insurance license, reserves, policies, policyholders, and claims. It is a formal way for business owners to self-insure against risk. Captives are usually formed to insure against the risks of one or more businesses owned by the same or related parties.

How does a captive insurance company work?

A captive primarily insures its parent company or related companies. Hence, the parent company is able to purchase insurance from its captive, and it can insure against risks that a third party insurer would either not insure or charge too much to insure. Premiums are paid from the parent

company to the captive with pre-tax dollars. The captive can invest its assets mostly as its owners choose (some domiciles have restrictions).

— Jonathan St. Clair, JD, and Ryan Manaker, SageView Advisory Group.

COMPLIANCE

What Anthem's HIPAA breach means to you

The massive data breach experienced on Jan. 29, 2015, by Anthem Insurance Companies, Inc. should serve as a wake-up call for all covered entities and business associates. In this situation, Anthem was both. Anthem is a covered entity to its members, or enrollees, and a business associate to other insurance plans when it processes claims for care delivered outside its covered areas.

Anthem, formerly known as Wellpoint, serves some 37.5 million members. Anthem participates in a larger organization, the Blue Cross Blue Shield Association (BCBSA). BCBSA offers the BlueCard, a networking arrangement that allows members to seek healthcare when traveling or living outside the service area of their health plan. When this happens, the provider submits the claim to the local Blues plan and then to the member's plan. This allows member's claims to be processed based on the member's personal plan.

Some 78.8 million individuals were affected in this breach, including Anthem enrollees, Anthem employees, and enrollees of other Blue Cross/Blue Shield plans, including Caremore, Empire BC/BS, and Unicare. The breach affected individuals in at least fourteen states, possibly more: California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New York, Ohio, Virginia, and Wisconsin.

Information that was compromised during the breach included the following patient details:

- Name
- Date of birth
- Social Security number
- Health care ID #
- Home and e-mail addresses
- Work information, such as income

Anthem officials stated that they do not believe that any credit card, banking, or medical information was included. However, the only information needed to illegally claim someone else's tax refund is their name, date of birth, and Social Security number.

There has been much speculation about the origin of this breach, as well as many accusations directed at Anthem. Some experts think the hacking goes as far back as Dec. 10, 2014, while others say that breaches may have occurred as far back as April 2014.

Anthem admitted that their data was encrypted only in transit, not at rest. However, because of the way their system was hacked, encryption would not have affected the breach.

This cyberattack may have been an inside job, but most likely, it was done by an outsider who obtained legitimate employee credentials by "phishing," that is, asking for sensitive information while pretending to be a trustworthy or otherwise legitimate entity. The attackers then used those credentials to access Anthem's database, bypassing firewalls and other security measures. This allowed the hackers to see unencrypted information, even if the data had been encrypted at rest.

A database administrator, a true Anthem employee, noticed that unauthorized queries were being run with administrator credentials. Anthem then started the investigation.

How could this attack have been prevented or mitigated? Experts describe two possibilities:

1. **Network Behavioral Analysis or Network Behavioral Anomaly Detection.** NBA or NBAD software perform automated, systematic behavioral analysis to detect unusual behavior. The software then raises red flags or disables access to protected networks. This software enhances security of a proprietary network, complementing but not replacing traditional security measures such as firewalls, intrusion detection systems, and antivirus software. It was a human being who spotted unusual behavior in the Anthem attack; NBA/NBAD

minimizes the time and labor required by depending on human operators. National Defender Plus is one example of NBA software.

2. **Context-Aware systems.** Context-Aware systems help monitor accesses that appear to be authentic, by detecting the geographical origin, the date and time of authentication, and which platform was used. It also tracks mobile devices.

Anthem breach Q&A

Q. What does the hack mean to affected individuals?

A. Possible identity theft is the fear, although there have been no reports that any affected individual has been victimized. Healthcare identity theft is huge, but at this time of the year, income tax refunds are the focus. The only information needed to falsely file for a tax refund is a name, Social Security number, and date of birth. Anthem has offered a free two-year subscription to AllClear ID, a service that provides "identity theft repair and credit monitoring." Few seem to have taken advantage of this offer, however.

Q. What does the hack mean to Anthem?

A. This breach could trigger heavy HIPAA-required fines in addition to administrative costs of contacting affected individuals and the costs for the identity theft protection service. At the time this was published, more than 50 class action suits had been filed and private suits are anticipated. Experts estimate that this incident alone could exceed $100 million; and some say up to $16 billion. Anthem declined to discuss any cap on their cybersecurity insurance. Cybersecurity insurance is a topic that DoctorsManagement continues to explore.

Q. What does this mean to you?

A. Every practice should recognize the urgency of protecting their electronic systems, whether at work or at home, whether they hold practice financial information, patients' protected health information, or their own personal information. This should also include protection for all mobile devices, which often pose the greatest risks.

If you have not already done so, here is a checklist of things to do in your practice to get you started:

- Develop and implement HIPAA policies and procedures.
- Train your staff.
- Work with your software vendors and IT support team to ensure that all needed security measures are in place and are current.

— Ann Bachman, CLC, MT (abachman@drsmgmt.com). The author is Director of OSHA, CLIA, and HIPAA Compliance at DoctorsManagement.

New DoctorsManagement clients	
Client	**Services provided**
Orthopedic practice, ME	Feasibility study
Single doctor, primary care	Practice start-up
Surgery practice, OH	Feasibility study
Orthopedic/sports medicine practice, GA	Practice assessment
Cardiology group practice, NY	Practice start-up
Internal medicine practice, MO	Contract review
Health system, IL	Credentialing
Dental group practice, TN	Regulatory compliance
Pain management group	Regulatory compliance
Laboratory group	Lab start-up
Primary care group	Lab and technical consulting
Health system, FL	Compliance consulting
Ongoing legal investigation	Litigation review, audit sampling/analysis
Hospital group, TN	Compliance risk analysis
Hospital system, GA	Compliance risk analysis
Health system, FL	Compliance risk analysis
Dermatology group, TN	Human resources consulting
Family practice, GA	Human resources consulting
Pediatric group practice, FL	Employee handbook review/editing
11 new clients for litigation review and audit sampling/analysis services	
17 new power buying clients	