The Coding Institute — SPECIALTY ALERTS
CodingInstitute.com; SuperCoder.com — *Helps Coders Help Physicians*

Part B Insider

News & Analysis on Part B Reimbursement & Regulation

2011, Vol. 12, No. 10 (Pages 73-80)

In This Issue

Annual Wellness Visits

G0438-G0439: MACs Share Additional Information About AWVs

Hint: You can perform AWVs on new patients.

Part B practices looking for answers about the new annual wellness visit (AWV) services that Medicare allows this year have come up short, with CMS still waiting to release more comprehensive coding guidance on the matter than the *MLN Matters* article that the agency issued months ago. But MACs have continued to share answers to the frequently-asked questions that they've received on the topic, and we've got a few of the answers to help you ensure that your G0438-G0439 claims process smoothly.

Question 1: Can we collect for an AWV that we perform on a patient we've never treated before?

Answer: Absolutely. "There is no regulation the patient has to be established," **WPS Medicare** notes on its Web site. The MAC, which is a Part B payer in four states, indicates that if the patient had an AWV at another practice during a prior year, you'll report G0439 (*Annual Wellness Visit, includes a personalized prevention plan of service [PPPS] subsequent visit*) for your service. If the patient has never had an AWV before, you'll bill G0438 *(...first visit*).

Question 2: What type of documentation does Medicare require for recording the AWV?

Answer: You'll want to document the AWV the same way you document all other services that your practice performs — thoroughly and carefully.

According to a directive on the Web site of **Trailblazer Health Enterprises**, a Part B payer in five states, "Physicians, qualified non-physician practitioners, and medical professionals are required to use the 1995 or 1997 E/M documentation guidelines to document the medical records with the appropriate clinical information. All referrals and a written medical plan must be included in the documentation."

Question 3: Is G0438 a "once in a lifetime" code?

Answer: Yes, you can only report G0438 once per beneficiary. If you submit a claim for G0438 and Medicare has already covered that beneficiary for another instance of that code, you'll receive an EOB with claim adjustment reason code 149 (*Lifetime benefit maximum has been reached for the service/benefit category*), according to Pinnacle Business Solutions, a Part B MAC in two states.

For our previous rundown of AWV frequently-asked questions, see the Insider, Vol. 12, No. 4. You can send your AWV questions to our editor Torrey Kim at torreyk@codinginstitute.com. ❑

Compliance

RAC 'Bounty Hunters' Turning Their Sights on Medicaid Claims

Fortunately, recent delays give you more time to plan for these audits.

If you thought you had already gotten your fill of recovery audit contractors (RACs) via your Part B claims, get ready for a whole new wave of audits. Thanks to last year's Patient Protection and Affordable Care Act, it looks like RAC auditors will soon be reviewing Medicaid claims as well.

In place for Medicare contractors since 2005, RACs are often referred to as medical "bounty hunters" because they only make money if they collect overpayments from you. Their income is specifically tied to the amount they recover, and is based on a percentage of the overpayments they identify.

"Medicaid RACs are tasked with identifying and recovering Medicaid overpayments and identifying underpayments," the CMS Web site notes. The agency sent a letter to each state's Medicaid director informing them of the RAC audit specifications (www.cms.gov/smdl/downloads/SMD10021.pdf). Initially, RACs were supposed to be in place by April 1 of this year, but that deadline has been extended, says **Mark W. Bina, Esq.,** with Krieg DeVault, LLP in Chicago.

"All states were required to have their RAC programs implemented by April 1," Bina says, "But most states were unable to meet this deadline because of various budgetary and operational hurdles. On February 1, CMS announced the deadline would be pushed back indefinitely."

The new implementation deadline has not yet been set but will be identified in a Final Rule to be published later in 2011, Bina says.

Prepare: Although the Medicaid RAC program has been postponed, it's a good idea to brush up on RAC facts before the audits hit. *For example:* If a RAC contacts you and indicates that an audit is imminent, you'll want to find out the deadline by which you're required to submit any requested records, as well as the point of contact for the audit.

Appeals: RAC determinations are not the final say regarding whether you'll owe money. State Medicaid programs will be required to have appeal processes in case your practice disagrees with a RAC's findings.

"Under the Proposed Rule related to the Medicaid RAC program, CMS proposed to permit states the 'flexibility to determine the appeals process that would be available to providers who seek review of adverse RAC determinations,'" says **Jessica L. Gustafson, Esq.,** with The Health Law Partners, PC in Southfield, Mich. "Significantly, this means that the appeals process will likely differ from state-to-state," she adds. ❑

Documentation

Do Your Providers Meet Signature Requirements on Their Charts?

Answers to 2 common questions help ensure you're on track.

Including provider signatures is a basic documentation requirement for your patient charts, but can also be a daily challenge. Check your answers against our experts' advice to verify your group's signature compliance.

Handwritten and Electronic Could Meet Criteria

Question 1: Some of our physicians use handwritten signatures on their charts and others prefer electronic signatures. Is either kind acceptable?

Answer 1: According to CMS documents, "Medicare requires a legible identifier for services provided/ordered." That "identifier" – or signature – can be electronic or handwritten, as long as the provider meets certain criteria. Legible first and last names, a legible first initial with last name, or even an illegible signature over a printed or typed name are acceptable. You're also covered if the provider's signature is illegible but is on a page with other information identifying the signer (letterhead, addressograph, etc.).

"Also be sure to include the provider's credentials," says **Cindy Hinton, CPC, CCP, CHCC,** founder of Advanced Coding Solutions in Franklin, Tenn. "The credentials themselves can be with the signature or they can be identified elsewhere on the note."

(Continued on next page)

Clip and Save

Use This Handy Chart to Remember What Equals a Signature

Steer clear of stamps.

Learning the ins and outs of what constitutes a compliant handwritten signature can be tricky, but isn't impossible. Compare your charts to these tips from **Judith Blaszczyk, RN, CPC, ACS-PM,** of Auditing for Compliance and Education in Leawood, Kan., and **Marvel Hammer, RN, CPC, CCS-P, PCS, ASC-PM, CHCO,** owner of MJH Consulting in Denver, Co., to determine if your group needs to update its signature strategy.

Signature Requirements Are Met	Signature Requirements Are Not Met
Legible full signature	Unsigned typed note with or without provider's typed or printed name
Legible first initial and last name	Unsigned handwritten note, only entry on the page
Illegible signature over a typed or printed name	"Signature on file" notation
Illegible signature where letterhead, addressograph, or other information on page indicates identity of signer	Illegible signature NOT over a typed or printed name and NOT on letterhead, unaccompanied by a signature log or an attestation statement
Illegible signature NOT over a typed or printed name and NOT on letterhead but accompanied by a signature log or an attestation statement	Initials NOT over a typed or printed name, unaccompanied by a signature log or an attestation statement
Initials over a typed or printed name	Stamped signature
Initials NOT over a typed or printed name but accompanied by a signature log or an attestation statement	
Unsigned handwritten note with other entries on same page, in same handwriting are signed	

Example: Pre-printed forms might include the physician's name and credentials at the top, side, or end. All qualify as acceptable documentation as long as the coder or auditor can identify the provider's credentials.

You can also use a signature log to back up your physician's documentation. The log should contain each provider's printed or typed name and credentials, along with their signatures and initials. You can reference the signature log in order to verify a note that contains an otherwise unidentifiable signature. "This is an important resource when providers are signing notes that do not include their typed or pre-printed name," Hinton says.

Tip: Update signature logs at least once a year. Create separate logs by provider (physicians, CRNAs, AAs, residents, etc.) to help simplify tracking.

Watch out: Stamped signatures don't meet the CMS requirements. Because a signature stamp can be used by anyone who has access to the stamp, in essence it doesn't authenticate that the billing provider was the author of the supporting documentation. You can, however, use a typed or printed block print name below the provider's signature to clearly identify an illegible signature.

Don't Let EMRs Do All Your Work

Question 2: Our office is in the process of switching completely to electronic medical records. Does that cover signature requirements for us?

Answer 2: Some coders – or providers – believe that electronic medical records (EMRs) do all the documentation work, but that's not necessarily the case. "Even electronic signatures must meet certain requirements," Hinton says. "Not all verbiage is created equal."

Considerations: As your providers incorporate EMR in their everyday care, double check the electronic signature's wording. Does it say, 'Electronically signed by' or 'Authenticated by'? Does it include the date? "There are numerous ways of phrasing and formatting the electronic signature," Hinton says. "Verify that the format you're implementing is approved by CMS."

Warning: "Electronic signatures carry the potential for misuse or abuse," says **Judith Blaszczyk, RN, CPC, ACS-PM,** of Auditing for Compliance and Education in Leawood, Kan. "System and software products should be protected against unauthorized modifications." Electronic capabilities should also comply with recognized standards and laws; check with your healthcare attorney and/or malpractice insurer to confirm compliance. ❑

Patient Privacy

Keep HIPAA Concerns at Bay With Simple Risk Analysis

Beware 'willful neglect' penalties up to $50,000 per violation now in effect.

If you think HIPAA compliance doesn't need to be a priority in these hectic times, take a look at the fines associated with "willful neglect" HIPAA violations, a category that went into effect Feb. 17.

Ouch: If the Department of Health and Human Services determines a willful neglect violation occurred — which essentially means you didn't identify and try to preempt the risk — you can get hit with fines starting at $10,000 per violation, says HIPAA compliance expert **Jim Sheldon-Dean,** director of compliance services for Lewis Creek Systems in Charlotte, Vt. "And that's if you correct the problem within 30 days," he adds.

"If a provider takes more than 30 days to correct the violation, then the fines start at $50,000 per violation," adds Sheldon-Dean.

Background: The HITECH Act implemented the heftier fines for Health Insurance Portability and Accountability Act privacy and security violations in February 2009, he notes.

It gets worse: Sometimes one problem gets counted as multiple violations, each one ringing up a stiff fine. The number of violations "can multiply very quickly," says Sheldon-Dean.

Nail Down the Essentials For Risk Analysis

You can stave off crippling fines by performing a thorough HIPAA risk analysis in order to comply with the security rule, if you haven't already. The first step in the risk analysis is to look at the "big picture" to identify potential risk points, Sheldon-Dean says.

HIPAA

'Willful Neglect' Violations May Eventually Expand to Stolen Laptops or Other Devices Containing Unencrypted PHI

It could happen, says HIPAA expert.

Willful neglect violations can lead to some humongous fines. And one of your practice's biggest vulnerabilities may be portable devices containing unsecured PHI, say experts (*see the article, "Keep HIPAA Concerns at Bay With Simple Risk Analysis" on page 76*).

"HHS hasn't formally made a determination that a lost or stolen laptop [or other device containing unencrypted PHI posing a significant risk of harm to an individual] represents willful neglect," observes consultant **Abner Weintraub** in Orlando, FL. **"**If HHS made such a finding, it would likely be that not encrypting the data would constitute the 'willful neglect.'"

That could happen considering that "HIPAA is a reasonableness standard," Weintraub says. "Covered entities are supposed to take reasonable precautions against reasonably anticipated risks." And that includes the potential for what have been widely reported thefts of laptops containing unencrypted PHI, he points out. "Laptop thefts are probably second to cell phone theft."

Don't be one of these: "If you look at research and surveys related to data and device thefts**,** a lot of organizations still don't encrypt health data or mortgage data, etc., that could harm individuals if it fell into the wrong hands," cautions Weintraub. ❑

Start by identifying what systems are holding onto electronic health information that contains PHI, including electronic health records and business files, Sheldon-Dean advises. "Look at how those systems move information within the entity, as well as to business associates outside the entity or to other entities for other purposes."

After identifying the risk points, do a more detailed risk assessment of your individual systems. You identify their specific risk points, as well as significance — and the likelihood that a problem will occur, and then address it, Sheldon-Dean instructs.

There are several ways to do the risk analysis assessment, he adds, but the simplest approach is to use a methodology defined by the National Institute of Standards and Technology special publication on risk analysis (http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf).

(Continued on next page)

Target These 2 High-Risk Areas

Some of the riskiest areas these days involve portable devices containing protected health information, warns Sheldon-Dean.

Little devices, big risks: "As devices get smaller and more portable, the potential for lost or stolen or misplaced data increases — and so does the risk for a breach," warns **Peter Arbuthnot**, regulatory analyst with American HealthTech in Jacksonville, Miss.

In fact, identity thieves view health information data as the "highest quality" available for their purposes, warns Sheldon-Dean.

Must do: "It's really important to secure the information on devices by encrypting it and also have the capability to remotely wipe the devices clean, including laptops," he advises. To accomplish the latter, you set the device so that the next time it's turned on, the device calls home over the Internet, Sheldon-Dean explains. Then the software can tell the device "you've been stolen," which causes the device to eliminate its data.

Unsecured e-mail is also high risk, says Sheldon-Dean. "Copies can be left on mail servers or in unsecured areas."

Solution: Based on the HITECH Act, says Sheldon-Dean, the proper ways to secure e-mail or other documents/systems/files/data are defined in guidance from HHS, available at: www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html.

Key: "If electronic data has been secured (encrypted), then the covered entity does not have to report a breach," says consultant **Abner Weintraub** with The HIPAA Group Inc. in Orlando, Fla. "The assumption is that properly encrypted data is useless to anyone who has it."

Watch Out For Remote Access

Remote access is another high-risk issue for providers that have staff or contractors who use computerized PHI offsite, says Sheldon-Dean.

For one, "the PHI may end up on networks or computers that aren't properly secured," Sheldon-Dean cautions. Or an employee's family members may view the information when they use the same computer. "Even if you make the remote connection secure, once the data is on someone else's computer — it's outside."

To avoid these risks, off-site workers should use a dedicated computer. And you can set it up so the person accesses data over the web securely without being able to save or print the information, he adds. "You can use something like Citrix to tunnel into the entity's systems and work on them remotely without actually bringing any persistent data into your remote computer," explains Sheldon-Dean.

That way, "you don't wind up with any temporary files on the remote machine."

Don't Forget A Crucial Compliance Step: Auditing

Skimping on the audit process can be a costly mistake. You have to make sure everyone is doing what's expected based on policies and procedures, including managing risks related to portable devices and remote access, says Sheldon-Dean.

Remember: The HITECH Act requires HHS to conduct random audits of various types of entities, he says. And whatever fines HHS collects from the audits will go into an audit fund to pay for additional audits. Thus, "once HHS gets going, the audits will ramp up quickly." ❑

Part B Coding Coach

Follow These 4 Quick Guidelines to Collect for Inhaler Education Claims

Learn what steps to take when provider charges for a Diskus demo.

One thing you should keep in mind when reporting for inhaler demo/evaluation is the type of device the provider is using, but don't stop with just that. Documentation requirements and qualifying modifiers are just as important when coding for inhaler services.

When you're confused why some payers would deny reimbursement for certain inhaler claims, the following ideas could guide you to a better understanding of how inhaler service codes work out.

94664 Is Your Ticket to Diskus Demo Pay

The Advair Diskus is an "aerosol generator." If the nurse/medical assistant taught someone to use an Advair Diskus — or any other diskus — you should report 94664 (*Demonstration and/or evaluation of patient utilization of an aerosol generator, nebulizer, metered dose inhaler or IPPB device*).

Example: A pulmonologist starts a patient with asthma (493.00, *Extrinsic asthma; unspecified or 493.20, Chronic obstructive asthma; unspecified*) on Advair. A nurse then teaches the patient how to use the Diskus. As per CPT guidelines, you should report 99201-99215 for the office visit and 94664 without a modifier, says **Alan L. Plummer, MD**, professor of medicine, Division of Pulmonary, Allergy, and Critical Care at Emory University School of Medicine in Atlanta.

In addition, CMS transmittal R954CP also indicates that modifier 25 (*Significant, separately identifiable E/M service by the same physician on the same day of the procedure or other service*) applies only to E/M services performed with procedures that carry a global fee, which 94664 does not have.

Nonetheless, many payers will only pay for the service if you append modifier 25 to the visit code. It's always best to check with your major insurers' policy first.

Bundle Dose in Teaching Session

The patient may administer medication dose during the teaching session. Both services (treatment + teaching) are bundled into one CPT: 94640 (*Pressurized or nonpressurized inhalation treatment for acute airway obstruction or for sputum induction for diagnostic purposes [e.g., with an aerosol generator, nebulizer, metered dose inhaler or intermittent positive pressure breathing [IPPB] device]*), so you shouldn't report them separately.

Why: The administration was performed as part of the demonstration/evaluation.

Separate Education? Finish It Off With Modifier 59

Suppose that during an outpatient visit, an asthmatic patient is wheezing and having difficulty breathing, which requires one or more bronchodilator treatments for intervention: 493.01 (*Extrinsic asthma; with status asthmaticus*); 493.02 (*Extrinsic asthma; with [acute] exacerbation*); 493.21, (*Chronic obstructive asthma; with status asthmaticus*); or 493.22 (*Chronic obstructive asthma; with [acute] exacerbation*). The patient didn't use his MDI device, nebulizer, etc., properly prior to visit, so he was given an education about the use of these devices after the treatment.

Code it: First, code 94640 (adding modifier 76, *Repeat procedure or service by same physician, to separate line items of 94640 for multiple treatments*) in addition to the appropriate E/M code without a modifier, unless the payer requires modifier 25 with the E/M. Then report 94664 with modifier 59 (*Distinct procedural service*), as the patient required additional instruction for his daily maintenance medication.

This is different from the medication provided for immediate intervention (94640).

In short: If the patient required separate education after receiving an inhalation treatment on the same day, you would bill both services (treatment + education), appending modifier 59 to 94664.

Logic: The Correct Coding Initiative (CCI) places a level-one edit on 94640 and 94664. So Medicare and payers that follow CCI edits may require modifier 59 on the component code (94664) to indicate that the teaching is a distinct procedural service from the inhalation treatment. It is key that the teaching was not part of the treatment for the patient, which would be one parallel encounter — teaching while treating. Note in the example, the teaching took place, separately, after the patient received their treatment, says **Barbara J. Cobuzzi, MBA, CPC, CENTC, CPC-H, CPC-P, CPC-I, CHCC,** president of CRN Healthcare Solutions, a consulting firm in Tinton Falls, N.J. One could break these services into two separate serial encounters, one after another.

Easy $16 Through Medical Necessity Support

If payers would not pay your 94664 claim, you would need to support it with documentation indicating medical necessity to reimburse the approximately $16 national rate (0.47 RVUs multiplied by 2011 conversion factor of 33.9764). For instance, you might need to state in the Plan of Treatment portion of the written record that the patient requires a teaching session on the use of his MDI, diskus, nebulizer, etc. In addition, don't forget to note why the session is needed. ❑

Physician Notes

OIG Offers Free, Pre-Written Presentation for Teaching New Physicians About Compliance

Plus: Respond to CERT requests ASAP, MACs say.

When your practice hires a new physician, the job of training the doctor on healthcare compliance may fall to more than one person in your practice, including the office manager, compliance officer, coder, and fellow physicians. But that job may be a little bit easier now that the OIG has created a ready-made presentation that teaches new physicians how to steer clear of fraud.

The presentation, entitled, "Avoiding Medicare and Medicaid Fraud and Abuse," covers the five main areas of Medicare abuse: the False Claims Act, Anti-Kickback Statute, Physician Self-Referral Statute, Exclusion Statute, and Civil Monetary Penalties Law.

For example, the PowerPoint presentation, which the OIG offers in a .pdf format, reminds new doctors that prohibited kickbacks include "cash for referrals, free rent for medical offices, and excessive compensation for medical directorships." It also reminds physicians that it's illegal to sell free samples, and that you should always consider gift reporting requirements when accepting gifts.

To read the entire presentation, along with a booklet for physicians' self-study regarding how to avoid Medicare and Medicaid fraud, visit http://oig.hhs.gov/fraud/PhysicianEducation/.

In other news…

You'll be bringing yourself to CMS's attention if you fail to respond to Comprehensive Error Rate Testing (CERT) medical review requests.

CMS staff will be making calls to providers that haven't responded to CERT requests for medical review, MACs Cahaba GBA, Noridian, Highmark, and Palmetto GBA say on their Web sites.

"Although you may have already received letters and telephone calls from the CERT contractor, these additional efforts by CMS to obtain adequate documentation may change your claim's status from 'improper payment' to 'proper payment,'" they say. "This will allow us to calculate a more accurate Medicare FFS error rate, while also reducing the amount of improper payments." ❑

part B insider

Published 45 times annually by *The Coding Institute Company*
Subscription rate is $297.

Torrey Kim, MA, CPC, CGSC
Editor-in-Chief
torreyk@codinginstitute.com

Mary Compton, PhD, CPC
maryc@codinginstitute.com
Editorial Director

Melanie Parker
melaniep@codinginstitute.com
Publisher

Jennifer Godreau, CPC, CPMA, CPEDC
jenniferg@codinginstitute.com
Content Director

The Coding Institute - 2222 Sedwick Drive, Suite #101, Durham, NC 27713 Tel: (800) 508-2582 Fax: (800) 508-2592 service@codinginstitute.com

Part B Insider (USPS 023-079) (ISSN 1559-0240 for print; ISSN 1947-8755 for online) is published weekly 45 times per year by The Coding Institute - an The Coding Institute LLC, 2222 Sedwick Drive, Suite #101, Durham, NC 27713. Subscription price is $297. Periodicals postage is paid at Durham, NC 27705 and additional entry offices.
POSTMASTER: Send address changes to Part B Insider, PO Box 50028, 2222 Sedwick Drive, Suite #101, Durham, NC 27713.

This publication has the prior approval of the American Academy of Professional Coders for 0.5 Continuing Education Units. Granting of this approval in no way constitutes endorsement by the Academy of the content. Log onto Supercoder.com/membersarea to access CEU quiz. To request log in information, e-mail customerservice@supercoder.com

AAPC CEU APPROVED

Comments? Suggestions? Please contact Torrey Kim, CPC, Editor-in-Chief, at torreyk@codinginstitute.com.