The Coding Institute
AVOID AUDITS . IMPROVE REIMBURSEMENT . REDUCE DENIALS . INCREASE REVENUE

Part B Insider

News & Analysis on Part B Reimbursement & Regulation

May 2016, Vol. 17, No. 18 (Pages 137-144)

In This Issue

E/M Services

CMS: You Needn't Hold Transitional Care Management Claims for 30 Days

Date of face-to-face service can now be your DOS.

Tracking your practice's transitional care management (TCM) services can be a documentation headache—after performing the face-to-face visit, you've had to track that patient for a month, and then remember to submit your claim after the 30-day period ends. Fortunately, you're no longer stuck watching the calendar before you send your TCM claims to Medicare, thanks to a policy change for 2016.

Background: Ever since Medicare established the TCM codes in 2013, practices have been pleased to have a way to bill for the practitioner's work helping a patient transition from an inpatient location to their home or other community setting. Because the TCM services cover 30 days of care, practices were initially advised to hold the claims and not bill the TCM services until after 30 days had passed. This made claim tracking difficult, because practices had to remember to submit the claim weeks after they actually administered a face-to-face visit.

Submit Claims Right Away

Fortunately, you've got some more leeway this year in terms of when you can submit your TCM claims. According to a *Transitional Care Management FAQs* document that CMS published on March 17, you no longer have to wait until 30 days have passed before you send your claim to the applicable MAC.

"The 30-day period for the TCM service begins on the day of discharge and continues for the next 29 days," CMS says in the document. "The date of service you report should be the date of the required face-to-face visit. You may submit the claim once the face-to-face visit is furnished and need not hold the claim until the end of the service period."

Faster reimbursement: Practices across the country are pleased about the new rules. In particular, practitioners will be glad that they could get paid two weeks earlier than in the past, says Coding Consultant **Donelle Holle, RN**. "It's good news as far as I am concerned."

Fee Schedule Explained Change

The updated advice stems from a little-noticed TCM adjustment printed in the 2016 *Physician Fee Schedule Final Rule*, which read, "Regarding TCM services, we are adopting the commenters' suggestions that the required date of service reported on

the claim be the date of the face-to-face visit, and to allow (but not require) submission of the claim when the face-to-face visit is completed" *(page 131 of the Fee Schedule)*.

Therefore, your practice can either submit your TCM claim on the date of the face-to-face visit—as is now allowed—or you can wait until later in the month, as you have done since 2013. You'll report the services using the following codes:

» 99495 – *Transitional Care Management Services with the following required elements: Communication (direct contact, telephone, electronic) with the patient and/or caregiver within 2 business days of discharge; medical decision making of at least moderate complexity during the service period; face-to-face visit, within 14 calendar days of discharge.*
» 99496 – *Transitional Care Management Services with the following required elements: Communication (direct contact, telephone, electronic) with the patient and/or caregiver within 2 business days of discharge; medical decision making of high complexity during the service period; face-to-face visit, within 7 calendar days of discharge.*

Keep the Two-Day Window in Mind

To report TCM services, you must initiate contact with the patient and/or his caregiver either in person, via email or by phone, within two days of the patient's discharge from the inpatient setting.

"Any attempts to communicate should continue after the first two attempts until they have directly interacted with the beneficiary or caregiver," says Part B MAC Cahaba GBA in its *Transitional Care Management Billing* fact sheet. "A voicemail or e-mail without a response **will not** meet the requirement for post-discharge communication. Providers may not bill for transitional care management if contact was not successful within **30 days** between the facility discharge and date of service for the post-discharge code."

Meet These Documentation Requirements

You should ensure that your TCM documentation includes the following information, according to Cahaba GBA's fact sheet:

» The date the beneficiary was discharged
» The date interactive communication with beneficiary or caregiver was established
» The date the face-to-face visit was furnished
» The complexity of the medical decision process (i.e.) moderate or high

The last documentation rule mentioned above is particularly important because it drives your code choice. If you're treating a patient with moderate complexity decision-making, you must report 99495 and see the patient within

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 LLC, 2222 Sedwick Road, Durham, NC 27713. Subscription price is $349. Periodicals postage is paid at Durham, NC 27705 and additional entry offices.

POSTMASTER: Send address changes to Part B Insider, 4449 Easton Way, 2nd Floor, Columbus, OH, 43219.

14 days of discharge. If, however, the physician notes a high complexity of decision-making for the patient, you should bill 99496 and document that you saw the patient within seven days of inpatient discharge.

Resource: To read the complete FAQs on Transitional Care Management that CMS published in March, visit www.cms.gov/medicare/medicare-fee-for-service-payment/physicianfeesched/downloads/faq-tcms.pdf. ❑

Compliance

3 Common HIPAA Breaches –And How to Avoid Them

As the OCR's Audit Phase 2 looms large, watch your practice's loopholes for these common HIPAA blunders.

Privacy and security are major players in the health care industry today, and many practices keep coming up short. HIPAA violations are rampant, and when protected health information (PHI) breaches occur, it can be disastrous for everyone involved.

Background: According to the Health Information Technology for Economic and Clinical Health Act (HITECH) final ruling, a HIPAA breach occurs when an individual's privacy and security are at risk because his or her PHI has been "accessed, acquired, used, or disclosed." After a breach has been identified, the U.S. Department of Health and Human Services (HHS) requires individuals to be notified under HIPAA.

The HHS mandates under HITECH that "HIPAA covered entities and their business associates provide notification following a breach of unsecured protected health information (HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414)."

If you are worried about a breach, you might want to consider these four questions based on the HIPAA criteria used in enforcing the Breach Notification Rule:

1. What type of information was lost and how large an impact would it be?
2. Who obtained the PHI, and how and to whom was it leaked?
3. Did anyone actually receive and see the data?
4. What did your practice do to lessen the effect of the lost PHI?

Since most breaches are accidental and relatively benign, guidelines for exceptions to the rule are available for providers to follow if an infraction is suspected. Here are a few examples:

» An employee might "unintentionally" give the wrong patient data to a physician, but the doctor realizes the error and doesn't access the PHI.
» Authorized workers might unwittingly transfer PHI to another "covered entity," but that worker sees the mistake and deletes the information.
» Authorized personnel believe that the PHI could not be conveyed to another source—for instance, patient data was mailed but is returned unopened due to a wrong address.

Prevention Is Key

Oftentimes, the data lost is pivotal to the livelihood of your practice and is on a grand scale, particularly if the nature and breadth of the HIPAA breach involves over 500 patients in your state.

In massive cases like these, your practice must alert the patients, the media, and the HHS Secretary. If this happens, the OCR posts your error on its breach portal, there is usually a fine, and the press can report your HIPAA infractions to the public—and once it's out there, it never goes away.

Primary causes of compromised PHI are theft, unauthorized access or disclosure, and hacking or IT incident. Deterring these types of issues can be daunting, especially with complicated regulations to follow, but prevention is critical to practice compliance as the new OCR Audit Phase 2 program ramps up.

Fortunately, there are many things that providers can do to address these breaches such as performing a risk evaluation, focusing on compliance shortcomings, and putting measures into place with the data gleaned from the analysis. The HHS even offers a risk assessment tool, but many physicians don't utilize it.

"Many physicians don't understand that this [risk analysis tool] is the first element in HIPAA security," says **Abby Pendleton, Esq.** of The Health Law Partners, P.C., in their Southfield, Michigan office. "This type

(Continued on next page)

of risk analysis is the starting point to find potential vulnerabilities and then put into place the appropriate safeguards. It is the stepping stone to implement HIPAA but not enough practitioners do it."

3 Major Breaches and How to Fix Them

Consider the following three common breaches along with expert tips on how to avoid them.

1. Theft. PHI is commonly adulterated when practice or partner technology, information, or paperwork is stolen. This could mean hardware plundered by thieves, including laptops, desktops, tablets, or mobile phones, but it also refers to the paper route—lifted paperwork, hard files, discs and film (x-rays or photography). Sadly, employees can steal PHI as well, recording patient data for their own personal gain. When this kind of HIPAA breach happens, the records of patients are often exposed and sold for profit.

Theft is one of the easiest HIPAA breaches to deal with and overcome. A good place to start is with the encryption of all your electronic devices, especially the phone you might dictate into or the tablet you carry around the office. These types of at-rest devices can be quickly pocketed by anyone that comes through your practice doors from patients to employees to the guy that delivers your lunch.

Performing a comprehensive background check on all your employees and business associates before hiring needs to be mandatory for added security. Your practice should impose strict disciplinary guidelines for both staff and business associates should you uncover this type of theft of materials or information.

We Want to Hear From You

Tell us what you think about *Part B Insider*.

• What do you like?
• What topics would you like to see us cover?
• What can we improve on?

We'd love to hear from you.

Please email **Kristin J Webb-Hollering** at **kristinwh@codinginstitute.com**

Are You Breach Bound?

A HIPAA-compliant BAA will help you avoid breach burn.

Unauthorized access and disclosure land many a practice in hot water annually. Oftentimes, this type of breach cannot be controlled by physicians and their certified staff, who diligently follow HIPAA protocols to the letter. Unfortunately, despite these providers' efforts to stay compliant, the errors can usually be traced to business associates, who either fail to acknowledge the rules or are unaware of them. Ensuring that your business associate agreements (BAAs) are enforced can help you avoid issues down the road.

Who's to blame?

"There is really no reason why a provider shouldn't have BAAs in place in 2016," says **Michael D. Bossenbroek, Esq.** of Wachler & Associates, P.C. in Royal Oak, Michigan. Though an occasional infraction might slip by now and then, setting up a firm BAA will likely help you dodge this common breach. The BAA helps enforce the principles of HIPAA, and partners who refuse to enter into this type of contract probably aren't worth your time.

"Providers need to give careful thought to identifying their business associates and making sure that they have a HIPAA-compliant BAA in place with those business associates," Bossenbroek says. "Providers aren't necessarily responsible for the actions of their business associates, but a failure to execute a BAA is an easy way to get pulled into a business associate's breach or failure to comply with HIPAA."

Consider This

A strong BAA should be a top priority with clearly defined procedures and policies, suggests a recent report from the OCR on HIPAA cybersecurity, which also highlights the difficulties "covered entities" continue to have with the loss of PHI in their relationships with ill-advised business associates.

"I am aware of at least two recent settlements announced by OCR (North Memorial Health Care of Minnesota/$1.55 million and Raleigh Orthopaedic Clinic, P.A./$750,000) where OCR's investigation revealed the providers did not have a business associate agreement in place with a business associate, and this was a big point emphasized by OCR in both cases," Bossenbroek says. "My advice is that providers need to take the business associate relationship seriously."

Resource: For more information on the OCR cybersecurity update, visit https://nysdental.org/blog/ocr-issues-hipaa-cybersecurity-update. ❑

2. Unauthorized Access or Disclosure. This culprit is a frequent contributor to breaches and can easily be remedied with proper staff education. It often arises when providers and their employees let their policies slip when transferring PHI to third parties like claims and collections companies, outside billers, and insurance carriers.

This could be a detailed phone message or fax about a patient to an unauthorized individual or business associate or emailing patient PHI to insurers for claims, but it also covers something as simple as displaying patient information without consent on the practice bulletin board in the waiting room. The combination of what can be related, who has access to it, and where the PHI can officially go is the focus of this breach.

Constantly re-educating staff about your privacy practices and ensuring that they understand that this is a big deal in regard to patient security and safety is essential. Another crucial detail is having an ironclad business associate agreement that protects you against partners who aren't always reliable. Lastly, when you go about enlisting outside resources, look for "sophisticated vendors that have very advanced HIPAA programs because smaller firms don't know what the HIPAA rules are," says Pendleton.

3. Hacking or IT Incident. Unfortunately, more often than not, practices think they are prepared but are actually technically vulnerable. This is where the risk assessment tool comes in handy to show you where hackers are most likely to strike.

"Hackers are a step ahead of private practices, and they [physicians] easily fall victim to them," says **Clinton Mikel, Esq.** of The Health Law Partners, in their Southfield, Michigan office. "If the OCR investigates and finds over 500 individuals were affected, the first thing they will look for is the security risk analysis."

Five key steps to take to ward off hackers are as follows:

- » Assess your HIPAA risk annually either with the HHS online tool or using a reputable firm or program.
- » "Hire a good IT firm who is well versed in the up-to-date HIPAA regulations and security issues. The expenditure is recommended because health care security is complex," suggests Mikel.
- » Test your software often for vulnerabilities and keep it updated.
- » Ensure that your tech people are monitoring the firewall security.
- » Look for antivirus products that protect against threats common to health care hacking.

Resources: For more information about breaches and the HIPAA Breach Notification Rule, visit www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

For a quick link to the HHS risk assessment tool, visit www.healthit.gov/providers-professionals/security-risk-assessment. ❑

Part B Coding Coach

Focus on These Updates to ICD-10 Codes for Eye Care Specialists

Here's a closer look at your coding options in Ophthalmology.

New and expanded diagnosis codes for suspected amblyopia, non-exudative age-related macular degeneration, retinal vein occlusion, and diabetic retinopathy are the highlights ophthalmology coders should look for when the next batch of ICD-10 revisions become effective this October.

Background: In March, the ICD-10 Coordination and Maintenance Committee released its list of new and revised ICD-10 codes for fiscal year 2017. The codes take effect for dates of service on Oct. 1, 2016, or later. Overall, the Centers for Disease Control and Prevention (CDC) and the Centers for Medicare & Medicaid Services (CMS) will introduce 1,900 new diagnostic codes.

New Diabetes Options That Matter

Many of the changes in ophthalmology diagnosis coding will be seen in the E08.3xx *(Diabetes mellitus due to underlying condition with ophthalmic complications)*, E09.3xx *(Drug or chemical induced diabetes mellitus with ophthalmic complications)*, E10.3xx *(Type 1 diabetes mellitus with ophthalmic complications)* and E11.3xx *(Type 2 diabetes mellitus with ophthalmic complications)* code series.

The expansion of these series will mostly be due to eye specificity – adding one extra digit to specify whether the right, left, both, or unspecified eyes are affected.

These ICD-10 codes already contain a great deal of detail, including which type of diabetes is present (Type 1 or Type 2), and the type and severity of the ophthalmic condition. Each additional character in the code adds more specificity.

For example, for Type 1 diabetes, you would start with the E10.3 series. From E10.3, you would move on to the fifth character, which describes the type and severity of the ophthalmic condition. (E10.31: unspecified diabetic retinopathy; E10.32: mild nonproliferative diabetic retinopathy; E10.33: moderate nonproliferative diabetic retinopathy; etc.)

The sixth character, if any, specifies whether or not macular edema is present *(*e.g., E10.331, *Type 1 diabetes mellitus with moderate nonproliferative diabetic retinopathy with macular edema.)*

The ICD-10 revisions for 2017 will, in many cases, add a seventh character to these codes, which will specify which eye is affected:

- Seventh character 1: Right eye
- Seventh character 2: Left eye
- Seventh character 3: Both eyes
- Seventh character 4: Unspecified eye

Example: Effective Oct. 1, 2016, ICD-10 code E08.321 *(Diabetes mellitus due to underlying condition with mild nonproliferative diabetic retinopathy with macular edema)* will no longer be valid. In its place, you will report one of these more specific codes:

- E08.3211 – *Diabetes mellitus due to underlying condition with mild nonproliferative diabetic retinopathy with macular edema, right eye*
- E08.3212 – … *left eye*
- E08.3213 – … *bilateral*
- E08.3219 – … *unspecified eye*.

More Specificity for RVO Dx

By contrast, the retinal vein occlusion codes already have specific characters explaining which eye is affected. The additional characters in those codes beginning Oct. 1 will specify whether macular edema or retinal neovascularization is present, or if the eye is stable.

Example: Before Oct. 1, you would report central retinal vein occlusion in the right eye with H34.811 *(Central retinal vein occlusion, right eye)*. After Oct. 1, that code will no longer be valid. Instead, report one of the following:

- H34.8110 – *Central retinal vein occlusion, right eye, with macular edema*
- H34.8111 – … *with retinal neovascularization*
- H34.8112 – … *stable*.

The same holds true for the tributary (branch) retinal vein occlusion (H34.83x) code series – you will add a seventh character (0, 1, or 2) to describe macular edema, retinal neovascularization, or stability.

Specify Side, Stage With New Wet or Dry AMD Codes

You will also see a dramatic expansion within the age-related macular degeneration (AMD) diagnosis codes. Currently, you have two to choose from, depending on whether the patient suffers from nonexudative (dry) or exudative (wet) AMD:

» H35.31 – *Nonexudative age-related macular degeneration*
» H35.32 – *Exudative age-related macular degeneration.*

On Oct. 1, 2016, ICD-10 will delete both of those codes, in favor of a series of more specific codes. The new codes add two characters on to the existing five characters, which will specify not only which eye is affected, but which stage.

The sixth character will specify the eye:

» 1: right eye
» 2: left eye
» 3: bilateral
» 9: unspecified.

The seventh character will represent the stage of the condition. For the dry AMD codes (H35.31), look for these seventh characters:

» 0: stage unspecified
» 1: early dry stage
» 2: intermediate dry stage
» 3: advanced atrophic without subfoveal involvement
» 4: advanced atrophic with subfoveal involvement.

For the wet AMD codes (H35.32), ICD-10 will introduce these seventh characters:

» 0: stage unspecified
» 1: with active choroidal neovascularization
» 2: with inactive choroidal neovascularization
» 3: with inactive scar.

Example: The patient is diagnosed with bilateral dry AMD with active choroidal neovascularization. Report ICD-10 code H35.3231 *(Exudative age-related macular degeneration, bilateral, with active choroidal neovascularization)*.

New Choices for Glaucoma, Amblyopia

The revisions to ICD-10 will not lengthen the primary open-angle glaucoma codes (H40.11xx), but they will add more specificity. The new codes will replace the current sixth character in these codes, an "X" placeholder, with one of four codes representing which eye is affected:

» 1: right eye
» 2: left eye
» 3: bilateral
» 9: unspecified.

Example: Prior to Oct. 1, you would report a diagnosis of severe-stage primary open-angle glaucoma with H40.11X3 *(Primary open-angle glaucoma, severe stage)*, regardless of which eye was affected. After Oct. 1, you would pick one of the following codes, which replace the "X" with the new sixth character representing a specific eye:

» H40.1113 – *Primary open-angle glaucoma, right eye, severe stage*
» H40.1123 – … *left eye, severe stage*
» H40.1133 – … *bilateral, severe stage*
» H40.1193 – … *unspecified eye, severe stage*.

In addition, four new codes will debut on Oct. 1 in order to identify and monitor suspected cases of amblyopia:

» H53.041 – *Amblyopia suspect, right eye*
» H53.042 – … *left eye*
» H53.043 – … *bilateral*
» H53.049 – … *unspecified eye.*

Background: The American Academy of Ophthalmology made the case for these codes to the ICD-10 committee last September. In most cases, with older patients, amblyopia – decreased vision in one or both eyes compared with normal vision – is documented with eye charts or fixation preference testing, notes the AAO.

However: With children, "In some cases it is hard to be certain of the diagnosis," the AAO claims. "For instance a young child is unable to read a chart but has refractive, strabismic, or eye structural problems that often are associated with amblyopia. While these conditions can be coded in some instances, the possible presence of amblyopia cannot be coded."

Solution: "The presence of these codes in the medical record and problem list would serve as a reminder that this child has significant risk factors that can be associated with permanent visual loss due to amblyopia," says the AAO. "A unique code would serve as a reminder so the child receives ongoing medical observation and timely intervention when required."

Resource: For more ICD-10 information, visit www.cms.gov/Medicare/Coding/ICD10. For a complete list of the ICD-10 additions, deletions, and revisions, visit http://1.usa.gov/22ZxeNI. ❑

Physician Notes

Review Your Data Before Open Payments Go Live on May 15

Plus: Chiropractor charged with laundering health care payments.

As the 45-day window closes on May 15 to review and dispute so-called "sunshine payments," CMS urges physicians and teaching hospitals to take a look before the information goes live to the public.

It's always a good idea to review the payments that drug, device, and biologic manufacturers claim to have paid you because if it's wrong you'll want to dispute it and have the data amended before it is available to the public on June 30, 2016.

"The public has searched Open Payments data more than 6.3 million times," CMS says in a blog post from April 14. That means that consumers are interested and likely applying the findings from the reports to their future searches for a reputable provider.

CMS will offer assistance via a live help desk this Saturday, May 14 and Sunday, May 15 from 8:30 a.m. to 7:30 p.m. (ET).

Resource: For more information about the CMS Open Payments Open Payments Physician and Teaching Hospital Review and Dispute Period, visit www.cms.gov/openpayments/.

In other news…

An Illinois chiropractor faces up to 20 years in prison, $500,000 in fines, and three years of supervised release after pleading guilty to charges of health care fraud and money laundering, states a May 11 U.S. Department of Justice press release.

The Granite City doctor is said to have submitted false claims upwards of $500k to Medicare and a plethora of other agencies and carriers for services never rendered. The investigation managed by the Southern Illinois Health Care Fraud Task Force deduced that she was actually travelling abroad for the dates of service in question.

The chiropractor also admitted that she transferred $12,000 of the collected funds, resulting in a charge of money laundering.

Resource: For more information on this case filed by the Department of Justice,

U.S. Attorney's Office, Southern District of Illinois, visit www.justice.gov/usao-sdil/pr/granite-city-chiropractor-pleads-guilty-healthcare-fraud-and-money-laundering. ❑

part B insider

Published 45 times annually by *The Coding Institute*
Subscription rate is $349.

Kristin J Webb-Hollering
Editor
kristinwh@codinginstitute.com

Mary Compton, PhD, CPC
maryc@codinginstitute.us
VP Publishing

Jan Milliman, MA
janm@codingistitute.com
Editorial Director

Leesa A. Israel, BA, CPC, CUC, CEMC, CPPM, CMBS
leesai@supercoder.com
Director, SuperCoder.com From The Coding Institute

The Coding Institute LLC, 2222 Sedwick Road, Durham, NC 27713 Tel: 1-800-508-2582 Fax: 1-800-508-2592 E-mail: service@codinginstitute.com

Comments? Suggestions? Please contact Kristin J Webb-Hollering, Editor, at kristinwh@codinginstitute.com.

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. To access each issue's CEU quiz, visit Supercoder.com/ceus and then login. To request login information, email password@supercoder.com

The CEU is valid for 1 year from issue's month.

AAPC CEU APPROVED