NOVEMBER 2023 | VOLUME 49 | NUMBER 21

tci Newsletters

MEDICARE COMPLIANCE & REIMBURSEMENT

Master Medicare's latest in 20 minutes.

In this issue

HIPAA

Don't Skimp On Sanction Policymaking, Feds Warn

Tip: Ensure employees receive training equivalent to their duties.

When a data breach occurs, there's more to an organization's mitigation duty than merely retrieving the records and stopping the incident. That's where a sanction policy comes into play. Your mitigation efforts must extend to the sanctions you levy on staffers who cause inappropriate protected health information (PHI) disclosures under HIPAA, regardless of their intent.

Context: According to the HHS Office for Civil Rights (OCR), a sanction policy is "an important tool for supporting accountability and improving cybersecurity and data protection," the agency maintains in the October 2023 *OCR Cybersecurity Newsletter*. "Sanction policies can be used to address the intentional actions of malicious insiders, such as the stealing of data by identity-theft rings, as well as workforce member failures to comply with policies and procedures, such as failing to secure data on a network server or investigate a potential security incident," OCR advises.

Not only is a sanction policy a useful device that lets employees know from the get-go that there will be consequences for noncompliance, but it's also a requirement under both the HIPAA Privacy and Security Rules. Cultivating an environment where employees understand their responsibilities to keep PHI secure while also feeling safe to report suspicious activity is critical to a successful HIPAA compliance plan.

Read on for advice on developing a sanction policy for your organization.

Allocate Sanctions That Are Fair and Applicable to the Level of Violation

Setting up a sanctions policy can be a tricky business. If the plan is too stringent, employees will be less likely to report incidents for fear of censure or job loss. However, if the consequences are too lenient, staff may not respect the rules with the loss of PHI or ePHI inevitable. As you design your policies, ensure that the penalty fits the violation.

"HIPAA requires 'appropriate sanctions,'" explains attorney **Shannon Hartsfield**, an executive partner with Holland & Knight LLP in Tallahassee, Florida. "Generally, it may not be appropriate to immediately jump to employment termination if someone makes an innocent mistake. If every little HIPAA misstep, no matter how unintentional, results in someone losing their job, no one is going to report problems that could otherwise be resolved or not allowed to fester."

An overly punitive sanction policy may curtail staff from coming forward when accidents happen, especially if management aren't held to the same standards. And when that happens, privacy and security may be impacted. For example, "it would not be appropriate to fire a lower-level worker without hesitation for something that the company's CEO has also done without being fired," Hartsfield cautions.

Open lines of communication and equitable policies elevate compliance, too, says HIPAA expert **Jim Sheldon-Dean**, founder and director of compliance services at Lewis Creek Systems LLC in Charlotte, Vermont. "Establishing trust and showing that the organization treats security issues fairly are key to organizational success with sanctions. Where there is found to be an intentional violation, disciplinary action is a learning moment for other staff, and where there is an accidental violation, it's a learning moment for the organization," Sheldon-Dean asserts.

"What can we do better to keep this from happening again? Make issues a positive, and praise those who find them, as well as fix them," he proposes.

Consider this: That's why dedicating time and money to create the training materials and educating staff on the HIPAA rules is important; subpar training may lead to compliance failures — and sanctions. "If training is lacking, the organization should look at who is responsible for the training, and whether sanctions are appropriate in that circumstance for not appropriately implementing HIPAA's training requirement," Hartsfield says. "The organization should also consider who is authorized to impose sanctions, and whether they truly have that authority within the organization."

She adds that additional education should be a part of the sanction policy, too. "Sometimes documented counseling is an appropriate sanction," Hartsfield expounds. "A sanction could involve re-training the people involved, or even looking at whether an entire department should be retrained to make sure that potentially systemic problems don't continue."

Sheldon-Dean agrees. "If it's accidental but the employee should have known, the incident needs examination as to the cause of the issue." He suggests asking, "Is there a training deficiency? Do systems or processes encourage such mistakes? How widespread a problem is this?"

However, "sanctions may be appropriate if an employee has already been warned about an accidental issue and nobody else is having the same problem," Sheldon-Dean maintains.

Not all HIPAA violations are the same; therefore, the how, what, where, and why of PHI/ePHI loss should factor into the sanction decision-making process. "A sliding scale can be a reasonable way to approach violations," Hartsfield

CONTACT INFORMATION

Kristin J. Webb-Hollering, BA, CPCO, Development Editor
Leesa A. Israel, BA, CPC, CUC, CEMC, CPPM, CMBS, AAPC Fellow, AAPC MACRA Proficient
Head of Publishing, Editorial & Technology
Bulk Sales: 800-508-1316
Subscriptions: 800-508-2582 **Fax:** 800-508-2592

Medicare Compliance & Reimbursement (ISSN 1948-9595) is published biweekly except weeks of: New Year's Day, MLK Day, Easter, Memorial Day, July 4, Labor Day, Thanksgiving, and Christmas by The Coding Institute LLC, 2222 Sedwick Rd, Durham, NC 27713. Subscription price is $449.

POSTMASTER: Send address changes to Medicare Compliance & Reimbursement, 4449 Easton Way, 2nd Floor, Columbus, OH, 43219.

Subscription is also available in electronic format.

This newsletter has prior approval from AAPC for 0.5 continuing education units for every two issues (0.5 CEUs per month). Granting of this approval in no way constitutes endorsement by AAPC of the content.

The CEU is valid for 1 year from the issue's publication month. CEUs are earned by taking an online quiz. One quiz per month (every two issues) will be available for this newsletter.

recommends. "Depending on the nature of the improper use or disclosure of PHI or other compliance failure, a lesser sanction for a first offense could be appropriate. Consequences could escalate from there."

That's why "every 'accidental' issue needs a careful evaluation to see what can be done within policies, procedures, and systems to encourage the correct behavior in the future," Sheldon-Dean says.

Factor Remote Work Into Your Sanction Plan, Too

The combination of remote work, the use of personal devices, and decreased IT budgets make it harder to regulate data security — and that makes implementing a sanction policy more complicated with additional elements to consider. Risk assessment and analysis are critical components of compliance planning, are required under the HIPAA rules, and can help you address the intersection of remote work and sanction policymaking, suggests Hartsfield.

"Covered entities should document the risks relating to remote work and how those will be mitigated. Covered entities can implement systems and processes to require secure connections when remote workers access PHI, and these entities should also be auditing and monitoring remote workers and how they comply with the policies and procedures," she says. "Sanctions may be required for noncompliance."

Tip: Employing security safeguards like multi-factor authentication from the start can thwart potential security issues

both in the office and for remote workers, Sheldon-Dean says. "This makes access more consistent across the organization for all roles, and simplifies a lot of IT headaches. If there are still policy violations, see if access can be tightened, and use the incident as a training moment," he advises.

Educate Staff on the Sanction Policy Immediately

Workers need to know upfront and preferably during training about what they'll face for HIPAA-related infractions. Onboarding materials should include an overview of the sanction policy.

Add HC3 Resources To Your Cybersecurity Toolkit

Whether you're a data security novice or have always prioritized cyber hygiene, you should bookmark the HC3 webpage and take advantage of the handy and timely federal guidance.

Lowdown: The Department of Health and Human Services (HHS) created the Health Sector Cybersecurity Coordination Center (HC3) to better implement provisions outlined in the Cybersecurity Information Sharing Act of 2015. HC3 focuses entirely on cybersecurity, data sharing, and threats in the healthcare sector. Additionally, HHS religiously updates the HC3 webpage with new products, initiatives, and alerts.

HC3 is broken down into three areas. Here is an overview with the definition for each category:

- Under "threat briefs," HHS "highlights relevant cybersecurity topics and raises the [healthcare and public health] HPH sector's situational awareness of current cyber threats, threat actors, best practices, and mitigation tactics."
- Under "sector alerts," the agency gives "high-level" updates on threats with the information targeted specifically for a technical audience. The resources provide defensive advice to combat current large-scale threats and vulnerabilities.
- Under "other products," HHS offers concise analysis and education on hot cybersecurity topics with alerts and white papers. Recent deep dives include a white paper on artificial intelligence and phishing; analysis and fixes for issues with SolarWinds software; and a white paper on the intersection of QR codes and phishing.

Bonus: For healthcare cyber historians, an archive of resources is available. Check out HC3 at www.hhs.gov/about/agencies/asa/ocio/hc3/index.html. TCI

"Everyone who is going to be interacting with PHI should be trained upon hiring," Hartsfield says. "The training should be tailored to their particular job responsibilities, and the training should include references to the sanctions policy."

Reminder: OCR allows practices free rein to design and implement their training programs and sanction policy; however, many practices don't have qualified staff to compile the HIPAA training resources nor the funds. One positive is that "HIPAA is flexible and scalable," Hartsfield says. "A good place to start would be with existing human resources policies."

Since OCR permits CEs to determine their own "sanction methodology" based on the scope and scale of their organizations, there's room for a nuanced approach to policymaking, the agency says in the *Cybersecurity Newsletter*. "Regulated entities may structure their sanction policies in the manner most suitable to their organization."

Bottom line: Once your sanction policy is in place, however, that doesn't mean HIPAA training and analysis end. Though standards must be followed and issues managed, compliance continues to evolve based on human error, new technologies, and more.

If issues continue to arise, Sheldon-Dean suggests you ask, "Why are the violations happening? Can we improve processes and remove the need for the violation?"

"In many ways the analysis is easier as systems become more integrated and accessed uniformly, but there will always be improvements to be made," he observes. "You need to enlist your staff to help you find the weaknesses in your processes and let them know they'll be rewarded, not punished, for finding flaws in the organization. As technologies and society change quickly today, you need to be flexible and forgiving while your staff and your organization catch up," Sheldon-Dean says.

Resource: Find the OCR newsletter at www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-october-2023/index.html. TCI

Part B Coding Coach

Eye Care: Sidestep Cataract Surgery Snafus With Documentation Advice

Tip: Beef up chart notes with knowledge of 5 critical items.

Because cataract surgery continues to be one of the most commonly performed surgeries, it remains a top audit target for all payers. If your practice performs cataract surgery, it may only be a matter of time before you get audited.

You can start preparing for this eventuality by reviewing your payer policies for specific documentation requirements and taking steps to make sure your medical records stand up to scrutiny. Minimize errors and omissions by reviewing the following rules and requirements and incorporating them into your cataract surgery pre-op workup checklist.

Know the Medical Necessity Rules

The Centers for Medicare & Medicaid Services (CMS) — and payers that follow Medicare guidelines — will cover the costs of medically necessary cataract surgery. For example, Palmetto GBA, a Medicare Part B carrier, considers lens extraction medically necessary and covered when one or more of these conditions exist:

» Cataract causing symptomatic impairment of visual function not correctable with a tolerable change in glasses or contact lenses, lighting, or nonoperative means resulting in specific activity limitations and/or participation restrictions including, but not limited to reading, viewing television, driving, or meeting vocational or recreational needs;

» Concomitant intraocular disease (e.g., diabetic retinopathy or intraocular tumor) requiring monitoring or treatment that is prevented by the presence of cataract;

- » Lens-induced disease threatening vision or ocular health;
- » High probability of accelerating cataract development as a result of a concomitant or subsequent procedure (e.g., pars plana vitrectomy, iridocyclectomy, procedure for ocular trauma) and treatments such as external beam irradiation;
- » Cataract interfering with the performance of vitreoretinal surgery; and/or
- » Intolerable anisometropia or aniseikonia, uncorrectable with glasses or contact lenses, exists as a result of lens extraction in the first eye (despite satisfactorily corrected monocular visual acuity).

Medicare will consider covering other conditions, as well, but you'll need documentation that supports medical necessity and is compatible with the accepted standards of medical care. So, you should seek coverage for those on a case-by-case basis by working with your payers.

Watch for this: Surgery is not deemed to be medically necessary purely on the basis of lens opacity in the absence of symptoms. Also, the Snellen visual acuity chart results should be documented and will be considered toward medical necessity — but they're not enough on their own.

"An evaluation of visual acuity alone can neither rule in nor rule out the need for surgery," Palmetto says in its Local Coverage Determination (LCD). "Visual acuity should be recorded and considered in the context of the patient's visual impairment and other ocular findings."

Now that you're familiar with medical necessity requirements, let's take a closer look at five criteria for cataract surgery.

1. Lifestyle Complaint Indicating Hindrance of ADLs

Providers must ask patients about their visual symptoms and the activities they have difficulty performing to help establish the need for cataract surgery. Documentation of a chief complaint that impacts an activity of daily living (ADL) — reading, viewing television, driving, or meeting vocational or recreational expectations — is a fundamental requirement for all payers, notes **Joy Woodke, COE, OCS, OCSR**, director of coding and reimbursement at the American Academy of Ophthalmology. Try to include the patient's own words in the note, where possible, and specify the eye(s) impacted.

Tip: Ensure the medical record describes specific symptomatic impairments of visual function resulting in specific activity limitations.

Check individual payer policies for specific documentation requirements related to patient symptoms. For example, do patient complaints recorded in the chart note suffice, or is the use of a patient questionnaire (e.g., VF-8R) form required?

2. Objective Evidence of Cataract

Most payers require a preoperative comprehensive ophthalmologic exam (or its equivalent components occurring over a series of visits). Ophthalmologists should perform and document all 12 eye exam elements, the degree of lens opacity, and the type and grade of cataract (i.e., 1-4+). Make sure they consider and document the status of any concomitant ocular diseases that are present that could possibly affect the patient's vision.

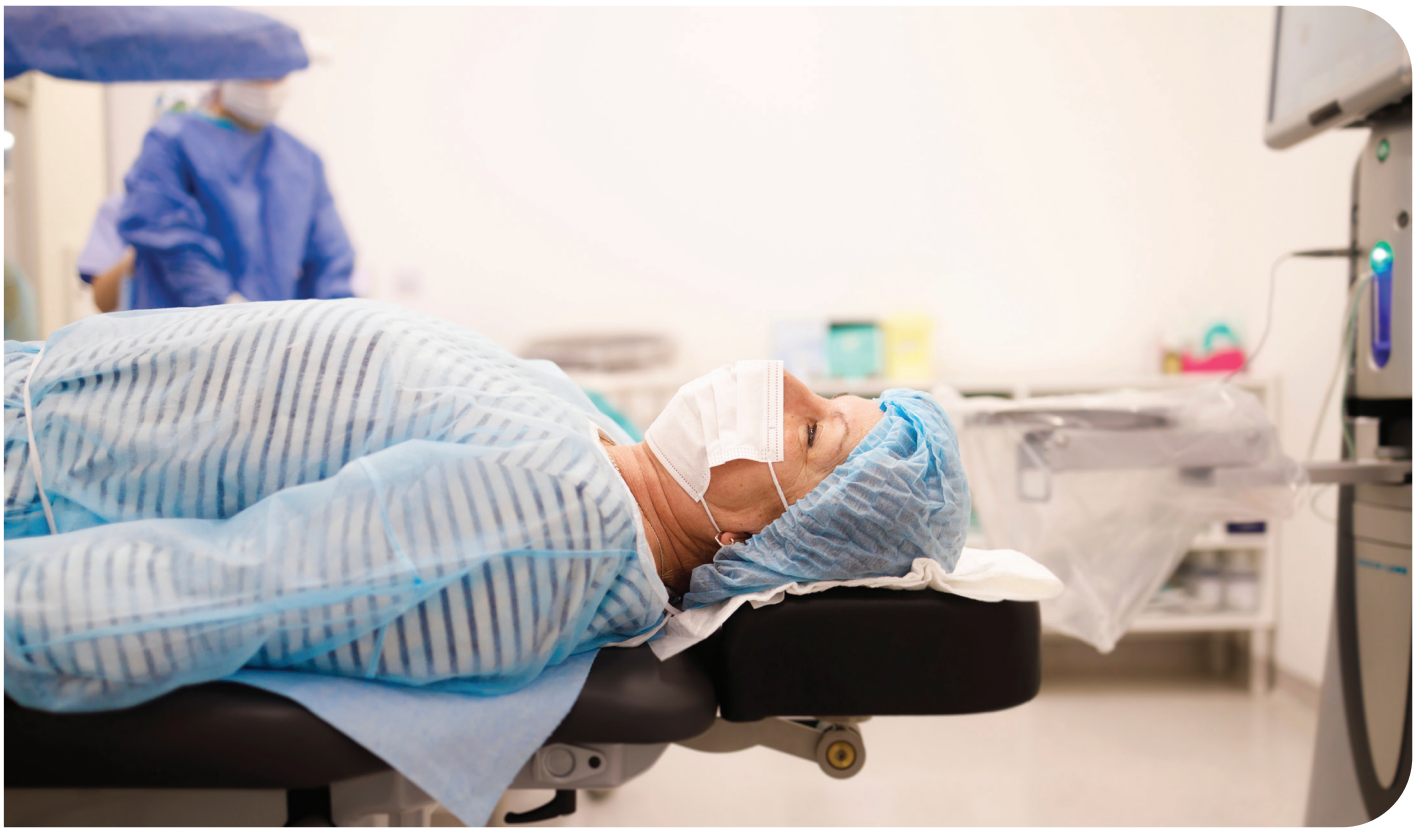
Tip: Have your providers include a statement in the medical record that they believe the cataract is significantly contributing to the patient's visual impairment.

3. Reduced Visual Acuity

Most policies want documentation of best-corrected visual acuity (BCVA), which requires a refraction. Patients may also need to undergo near vision and glare testing, both with uncorrected VA and BCVA, when indicated by the chief complaint. When they do, best practice is to document the method of glare testing.

"Some payers may allow an auto-refraction, while others will require a manifest refraction. Likewise, some allow surgeons to use a recent refraction provided in incoming records from a referring doctor, while others require the refraction be done in the surgeon's office," notes **Mary Pat Johnson, CPC, CPMA, COMT, COE**, senior consultant with Corcoran Consulting Group.

Glasses aren't an option: An indication that surgery may be necessary is when the patient's vision cannot be improved with a tolerable change in eyeglasses. So, you should include a statement by the surgeon in the documentation confirming that a change in glasses or contacts does not provide satisfactory functioning vision and the patient's lifestyle is compromised. Many payers require such a statement.



4. Good Prognosis for Improvement

Often, patients present with multiple ocular conditions that affect the patient's vision. Cataract surgery is warranted when other ocular diagnoses have been ruled out as the source of the decreased vision. A physician's attestation should indicate that the cataract is believed to be significantly contributing to the patient's visual impairment and that lens surgery will significantly improve both the visual and functional status of the patient.

5. Informed Consent and Anesthesia

In addition to a cataract diagnosis, recommendation for surgery, and attestation that there's a reasonable expectation that surgery will improve visual function, payers also expect documentation that the patient has been educated by the surgeon about the risks, benefits, and alternatives to cataract surgery, has provided consent, and desires to proceed with the operation. It's also important to note that the patient can tolerate anesthesia, and their awareness is sufficient to provide informed consent for surgery.

Prioritize Making Your Charts Audit-Proof

Over the past few years, ophthalmic practices around the country have received notification of Targeted Probe and Educate (TPE) audits and Supplemental Medicare Review Contractor (SMRC) audits focused on claims for cataract surgery (*see story, p. 7*). "More recently, CMS began sending Comparative Billing Reports focused on cataract-related services. In responding to these requests, pay close attention to the instructions in the LCD for your Medicare contractor. Review and adhere to the items noted in the Indications for Coverage section as well as the Documentation Requirements section of your policy," advises Johnson.

Note that while Medicare policies include many of the same elements, some provide more restrictive instructions on how the information needs to be documented.

Tip: Instead of trying to keep up with the different guidelines set forth by various payers, implement a single protocol for all payers — consider employing a procedure that meets the criteria outlined in your most restrictive policy to help ensure your charts can withstand payer scrutiny.

Lastly, ensure you're in compliance by performing internal chart audits.

Resources: Check out Noridian Medicare's Cataract Surgery Policy Checklist at https://med.noridianmedicare.com/documents/10546/27061036/Clinician+Checklists+Cataract+Surgery. Review CMS guidance on documentation and coding at www.cms.gov/medicare-coverage-database/view/article.aspx?articleId=57196&ver=17. TCI

Compliance

Cataract Surgery Remains Popular Medical Review Topic

Find out the codes the MACs are targeting in their TPE reviews.

Cataract surgery claims continue to sit atop auditors' to-do lists. And because that scrutiny doesn't seem to be going away any time soon, you may want to review the codes they're looking at as well as the probe results from recent prepayment claims reviews.

TPE: Over the past year, most of the Medicare Administrative Contractors (MACs) have either completed Targeted Probe and Educate (TPE) probes of cataract removal claims or have added them to their active topic lists. The specific code(s) included in the audit depends on the MAC and can vary, but the following CPT® codes are ones to know:

- **66821** (*Discission of secondary membranous cataract (opacified posterior lens capsule and/or anterior hyaloid); laser surgery (eg, YAG laser) (1 or more stages)*)
- **66982** (*Extracapsular cataract removal with insertion of intraocular lens prosthesis (1-stage procedure), manual or mechanical technique (eg, irrigation and aspiration or phacoemulsification), complex, requiring devices or techniques not generally used in routine cataract surgery (eg, iris expansion device, suture support for intraocular lens, or primary posterior capsulorrhexis) or performed on patients in the amblyogenic developmental stage; without endoscopic cyclophotocoagulation*)
- **66983** (*Intracapsular cataract extraction with insertion of intraocular lens prosthesis (1 stage procedure)*)
- **66984** (*Extracapsular cataract removal with insertion of intraocular lens prosthesis (1 stage procedure), manual or mechanical technique (eg, irrigation and aspiration or phacoemulsification); without endoscopic cyclophotocoagulation*)

Currently, this is the status of MAC audits by jurisdiction for cataract removal claims:

- **CGS Medicare:** The Part B MAC, which operates in jurisdiction 15, is doing prepayment TPE reviews of cataract surgery claims using codes 66821, 66982, and 66984.
- **First Coast Service Options:** FCSO, jurisdiction N's Part B MAC, has CPT® codes 66982-66984 on its TPE active agenda.
- **National Government Services:** NGS Medicare, the Part B carrier for jurisdictions 6 and K, is specifically focusing its TPE audits on the extracapsular cataract removal code 66984.
- **Noridian Healthcare Solutions:** Under Part A, Noridian conducted TPE audits for both jurisdictions E and F of cataract claims, posting results in July and August.
- **Novitas:** The MAC for jurisdictions JH and JL lists active TPE audits under both Part A and B for CPT® codes 66982-66984.
- **Palmetto GBA:** Under jurisdiction M, Palmetto added prepayment probe results for CPT® code 66984 to its website in August. The Part B MAC is also in charge of jurisdiction J and started performing TPE reviews of outpatient claims for 66984 in that area as of Aug. 18.
- **WPS Government Health Administrators:** According to its webpage, the Part A/B MAC, which operates in jurisdictions J5 and J8, is not auditing cataract surgery codes or claims via the TPE program at this time.

RACs: The Centers for Medicare & Medicaid Services (CMS) added cataract surgery claims to its approved audit issues for Recovery Audit Contractors (RACs) in 2017. According to both Cotiviti and Performant, the RACs continue to investigate cataract surgery claims problems in all regions.

CERT: Last December, CMS published the 2022 Medicare Fee-for-Service Supplemental Improper Payment Data as part of its Comprehensive Error Rate Testing (CERT) program. "Eye procedures" defined as cataract removal/lens insertion claims had an error rate of 8.3 percent and accounted for more than $146 million in improper payments, according to Table D1: Top 20 Service Types with Highest Improper Payments: Part B of the 2022 CERT report.

CMS noted that 100 percent of the issues were due to insufficient documentation. The 2023 CERT report is expected by the end of the year. TCI

Industry Notes

Use The Updated CMS-855I Form, MAC Reminds

If your practice is still using paper applications to enroll or update Medicare provider enrollment, know that the old CMS-855I or CMS-855R forms won't be accepted after Nov. 1.

Background: Though the Centers for Medicare & Medicaid Services (CMS) prefers that you enroll and update your information electronically through the Medicare Provider Enrollment, Chain, and Ownership System (PECOS), some providers continue to use paper forms and snail mail. Previously, physicians and nonphysician practitioners (NPPs) could use either the CMS-855I or CMS-855R to enroll and make corrections. However, CMS combined the two forms into a revamped CMS-855I and discontinued the CMS-855R; plus, the agency stopped taking the old forms on Oct. 31, 2023, reminds Part A/B Medicare Administrative Contractor (MAC) National Government Services in an Oct. 16 alert.

On top of combining the forms, CMS also added these features, NGS indicates:

- Physician specialties
- PA arrangements under reassignment section
- Telehealth expansion
- Compact licenses

NGS offers enrollment advice, YouTube videos on the subject, and a webinar on Nov. 10 explaining how to fill out the CMS-855I form. Review the news item at www.ngsmedicare.com/web/ngs/news-article-details?selectedArticleId=9857751&lob=96664&state=97178&region=93623&rgion=93623.

House GOP Doctors Aim To Bump Up CF By 2025

Budget neutrality mandates are at the heart of the annual Medicare conversion factor crunch. But congressional leaders want to change that and add some more money to your wallet in 2025.

Refresher: In the latest Medicare Physician Fee Schedule (MPFS) proposed rule published last July in the *Federal Register*, the Centers for Medicare & Medicaid Services (CMS) proposed to cut the calendar year (CY) 2024 conversion factor by 3.34 percent (see *Medicare Compliance & Reimbursement*, Vol. 49, No. 15).

Now: On Oct. 18, the House GOP Doctors Caucus announced legislation to change the threshold for updating budget neutrality. "The draft legislation would update the current $20 million budget neutrality threshold under the [M]PFS to $53 million in 2025," notes McDermott+Consulting, an affiliate of law firm McDermott Will & Emery, in a summary of the legislation. "The $53 million threshold would then be updated by an inflationary factor — the Medicare Economic Index — every fifth year starting in 2030."

Other key pieces of the legislation include:

- Mandating a lookback period.
- Ensuring CMS use the most reliable data when calculating the payment changes.
- Updating direct costs every five years to better calculate relative value units (RVUs).

Peruse the draft legislation at https://wenstrup.house.gov/uploadedfiles/pfs_discussion_draft.pdf. TCI