October 3, 2022 | Volume 36, Issue 38

Part B News
partbnews.com
COLLECT EVERY DOLLAR YOUR PRACTICE DESERVES

In this issue

decisionhealth
an hcpro brand

Practice management

Conduct regular checkups of your provider's public claims data

Use publicly available claims data to get a complete picture of your providers' data, see how they stack up against their peers and identify problems before they catch an investigator's attention.

The recent data brief from the HHS Office of Inspector General (OIG) on telehealth services during the first year of the COVID-19 public health emergency serves as a reminder that claims data is readily available.

It should be a call to action to review that data, says Sara Shanti, partner with Sheppard Mullin in Chicago (*PBN 9/26/22*). In addition, data review should be a regular part of a practice's risk-reduction plan.

"I really think doctors, just like they would recommend checkups to their patients, they should be doing data checkups for themselves," says Stephen Lee, solo practitioner, Law Office of Stephen Chahn Lee, LLC d/b/a Stephen Lee Law, Chicago. Lee's practice focuses on health care fraud and data analytics in litigation.

Understand who else looks at your data

In addition to providers who want to see how they stack up against their competitors, people who are looking for potential *qui tam* claims also mine the data, Shanti says. But investigators may be the most frequent users of claims data.

Claims data isn't the only element in a fraud investigation, but it plays a significant role. Lee regularly used claims data at the start of investigations when he worked for the health care fraud unit for the U.S. Attorney's Office for the Northern District of Illinois.

"When I got a new tip, I would pull the data and say 'OK, what's weird?'" Lee says. He would look at the code that made the provider the most money. "For a lot of practice[s], that's office visits. If I saw the number one code by dollars paid is something else, I would look at that." He would also use claims data to compare the provider who was the subject of the tip to other providers.

For example, there was the case of an Illinois dermatologist whose claims for **17004** (Destruction [eg, laser surgery, electrosurgery, cryosurgery, chemosurgery, surgical curettement], premalignant lesions [eg, actinic keratoses], 15 or more lesions) were much higher than his peers, Lee recalls. The investigation revealed that the dermatologist was using the code to report cosmetic light treatments. "As shown at the trial, lab techs were told to make up the numbers of alleged lesions that they destroyed — there was a template form with a blank for the number, and they were told to just put down a number greater than 15, which resulted in the highest billing code," Lee says. That case ended in a criminal conviction for the dermatologist.

Don't fear the data

The focus of a regular data checkup isn't to find things that the provider is doing wrong. A provider's numbers may look fine, or a provider may be an outlier for a legitimate reason including the nature of their patient population or the services they provide. "Someone has to be the number one biller in the country. That doesn't mean you're doing something wrong," Lee says.

If a provider is an outlier, that can serve as a reminder to make sure their documentation supports their claims. And if a practice discovers there is a problem, it is better to address it early and show the government you want to do the right thing, Lee says.

The data also will give you insight beyond the information your practice has. If a doctor or qualified health care professional does work for another provider, you'll be able to see those claims too.

"There are a lot of doctors who pick up a little side job, and I think a lot of the doctors don't realize that every time they sign an order that's another claim," Lee says. CMS' claims data gives the practice and provider the complete billing pattern that an investigator would see.

"I can look at your practice and tell you what the government would think of you," Lee says.

Finally, the data can reveal claims for services that the provider did not perform, which could be a sign of data theft.

Dig into the data

Thanks to CMS' public data sets, practices can review their own claims to see if anything looks weird

decisionhealth an hcpro brand

SUBSCRIBER INFORMATION

Have questions on a story? Call or email us.

***PART B NEWS* TEAM**

Maria Tsigas, x6023
Product Director
mtsigas@decisionhealth.com

Marci Geipe, x6022
Senior Manager, Product and Content
mgeipe@simplifycompliance.com

Richard Scott, 267-758-2404
Content Manager
rscott@decisionhealth.com

Roy Edroso, x6031
Editor
redroso@decisionhealth.com

Julia Kyles, CPC, x6015
Editor
jkyles@decisionhealth.com

Medical Practice & Hospital community!

www.facebook.com/DecisionHealthPAC
www.twitter.com/DH_MedPractice
www.linkedin.com/groups/12003710

SUBSCRIPTIONS
Direct questions about newsletter delivery and account status, toll free, to 1-855-CALL-DH1 or email: customer@decisionhealth.com

DECISIONHEALTH PLEDGE OF INDEPENDENCE:
Part B News works for only you, the provider. We are not affiliated with any special interest groups, nor owned by any entity with a conflicting stake in the health care industry. For nearly three decades, we've been independently watching out for the financial health of health care providers and we'll be there for you and your peers for decades to come.

CONNECT WITH US
Visit us online at: www.partbnews.com.

CEUS
Part B News offers prior approval of the American Academy of Professional Coders (AAPC) for 0.5 CEUs for every other issue. Granting of this approval in no way constitutes endorsement by the Academy of the program, content or the program sponsor. You can earn your CEUs by passing a five-question quiz delivered through the *Part B News* CEU website (https://ceus.coursewebs.com).

ADVERTISING
To inquire about advertising in *Part B News,* call 1-855-CALL-DH1.

Part B News® is a registered trademark of DecisionHealth. *Part B News* is published 48 times/year by DecisionHealth, 5511 Virginia Way, Suite 150 | Brentwood, TN 37027. ISSN 0893-8121. pbncustomer@decisionhealth.com Price: $677/year.

and compare themselves to their peers (*see resources, below*).

Lee provided a walkthrough of how to perform a quick utilization checkup with the "Medicare Physician & Other Practitioners — by Provider and Service" file:

1. Open the data set, select "View Data" and select the year you want to review. You can find this data set on the data.cms.gov website (*see resources, below*). The current data set includes files from 2013 to 2020.
2. Use the filter function to select your provider's top code. Select "HCPCS_Cd" in the first box, "Equals" in the next box and enter the code in the third box.
3. Select "Apply Filter." You'll get a list of every provider who billed that code for the given year, including their national provider identifier, name and address.
4. Scroll across to Total_Srvcs and click on that twice to create a descending list.

At this point you can use the export function to create a spreadsheet that you can save and review. However, it could be helpful to first narrow down the results to providers of the same specialty in the same state or city. Use the Advanced Filter function, which includes And/Or commands to select the specialty (Rndrng_Prvdr_Type); state using the postal abbreviation (Rndrng_Prvdr_State_Abrvtn); city (Rndrng_Prvdr_City); or five-digit ZIP code (Rndrng_Prvdr_Zip5).

If you want to reduce the number of columns in your results, use the "Manage Columns" function.

If you want to review or compare your providers' total payments, use the "Medicare Physician & Other Practitioners — by Provider" data set. The file includes the total dollar amount billed to and paid by Medicare for each provider for the year.

If you need help decoding the column abbreviations, each data set includes a dictionary as well as a methodology that explains how CMS calculates the data.

A quick look at your data can help you decide whether you need to dig a bit more, take action to address a problem or move on to another task. But if you don't look at your data, rest assured that someone else will.

"Lots of doctors out there have no idea how their Medicare data looks to the government and the public," Lee says. "I wish more people thought about this." — *Julia Kyles, CPC* (*jkyles@decisionhealth.com*) ■

RESOURCES

- Medicare Physician & Other Practitioners data sets: https://data.cms.gov/provider-summary-by-type-of-service/medicare-physician-other-practitioners
- Medicare Physician & Other Practitioners - by Provider and Service data set: https://data.cms.gov/provider-summary-by-type-of-service/medicare-physician-other-practitioners/medicare-physician-other-practitioners-by-provider-and-service
- Medicare Physician & Other Practitioners - by Provider data set: https://data.cms.gov/provider-summary-by-type-of-service/medicare-physician-other-practitioners/medicare-physician-other-practitioners-by-provider
- Chicago dermatologist conviction – Department of Justice press release: www.justice.gov/usao-ndil/pr/chicago-dermatologist-convicted-federal-fraud-charges-billing-health-insurance-programs

PBN Perspectives

Risk analysis initiated: Use updated assessment tool to stay safe

One major part of complying with HIPAA is conducting a risk assessment, and a new release from federal agencies gives you a fresh tool to perform an internal security risk assessment (SRA).

On June 14, OCR announced version 3.3 of the HHS Security Risk Assessment Tool. According to OCR officials, this tool is designed to aid small and medium providers in their efforts to assess security risks. The revamped tool contains a slate of new features, including Health Industry Cybersecurity Practices (HICP) references, file association in Microsoft Windows, improved reports, and other bug fixes and stability improvements.

The SRA Tool Excel Workbook is another new addition that the OCR calls an alternative version of the SRA Tool. It takes the same content from the Windows desktop application and presents it in a familiar spreadsheet format.

The workbook contains conditional formatting and formulas to calculate and help identify risk, similar to the SRA Tool application. It is intended to replace the legacy "paper version" of the tool and may be a good option for users who do not have access to Windows or

otherwise need more flexibility than is provided by the desktop application, according to OCR officials.

Examine resources for security risk analysis

Providers should note that the government landing page for the SRA Tool also features a wide variety of related information on HIPAA privacy and security, according to Frank Ruelas, MBA, a compliance professional located in Casa Grande, Ariz. This information includes videos, information sheets and other resources, as well as a user's guide for the tool. OCR has also created a website that provides "Security Rule Guidance Material."

"I think that covered entities [CE] should become familiar with the information provided on [these websites] because it will help them understand what is expected in terms of completing a risk analysis, which they can then apply to their use of the tool," he says.

Ruelas also notes that the SRA Tool is comparable in many ways to other tools he's seen. "I didn't notice anything much in the way of any features or anything in the user interface that made this tool very different to other tools," he says. "This can be a plus given that if people have used other tools, they likely will be able to use this one without too much difficulty."

Who should lead use of the SRA Tool?

Someone who can speak to their organization's current privacy and security practices should use and complete the tool, Ruelas says. This increases the likelihood of achieving a comprehensive accounting of the organization's processes and policies, he adds.

"When completed, users of the tool can see how well their current security practices are presented by the tool and use this to determine what, if any, changes or modifications to their current security practices may be needed," he says.

Ins and outs of the updated tool

The updated SRA Tool installed quickly and easily after being downloaded from the website, Ruelas reports. A disclaimer states that it is for "informational purposes only" and that use of the tool does not guarantee compliance with federal, state or local laws.

"In this sense," Ruelas adds, "the user of the tool should have some type of familiarity with the risk analysis process so as to use it in a way that will create a risk analysis that will meet the HIPAA Risk Analysis requirement within the Security Rule."

The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of electronic protected health information (ePHI), OCR officials wrote in guidance on risk analysis on their website. Risk analysis is the first step in that process.

"We understand that the Security Rule does not prescribe a specific risk analysis methodology, recognizing that methods will vary dependent on the size, complexity, and capabilities of the organization," OCR writes. "Instead, the rule identifies risk analysis as the foundational element in the process of achieving compliance, and it establishes several objectives that any methodology adopted must achieve."

Same three-step process

The SRA Tool uses the same three-step approach as previous versions and is, overall, well laid out and logically presented, Ruelas says.

"These steps include entering some basic information about the organization, assessing different threats and vulnerabilities, and generating what is often referred to as a risk register, which is used in the risk management portion of the Security Rule to identify where risk mitigation strategies may be needed," he says.

Information in tool needs to be solid

When using the SRA tool, the quality of the output will only be as good as the information inputted, Ruelas says.

"I think that, at a minimum, one should review the tool's user guide and become familiar with how to use the tool," Ruelas says. "In this way, a user will be able to focus on the task at hand of entering valid responses into the tool so as to create meaningful output, which may identify actionable responses rather than having to be distracted on how to use the tool itself."

Which security risk assessment tool to use?

You may want to test out the tool before deciding it's the right one for you, Ruelas suggests.

(continued on p. 6)

Benchmark of the week

One obstacle for more advanced med tech adoption: Malpractice

One critical factor in physicians' decisions to use new medical technology is a concern that the new tech may expose the physician or practice to liability claims.

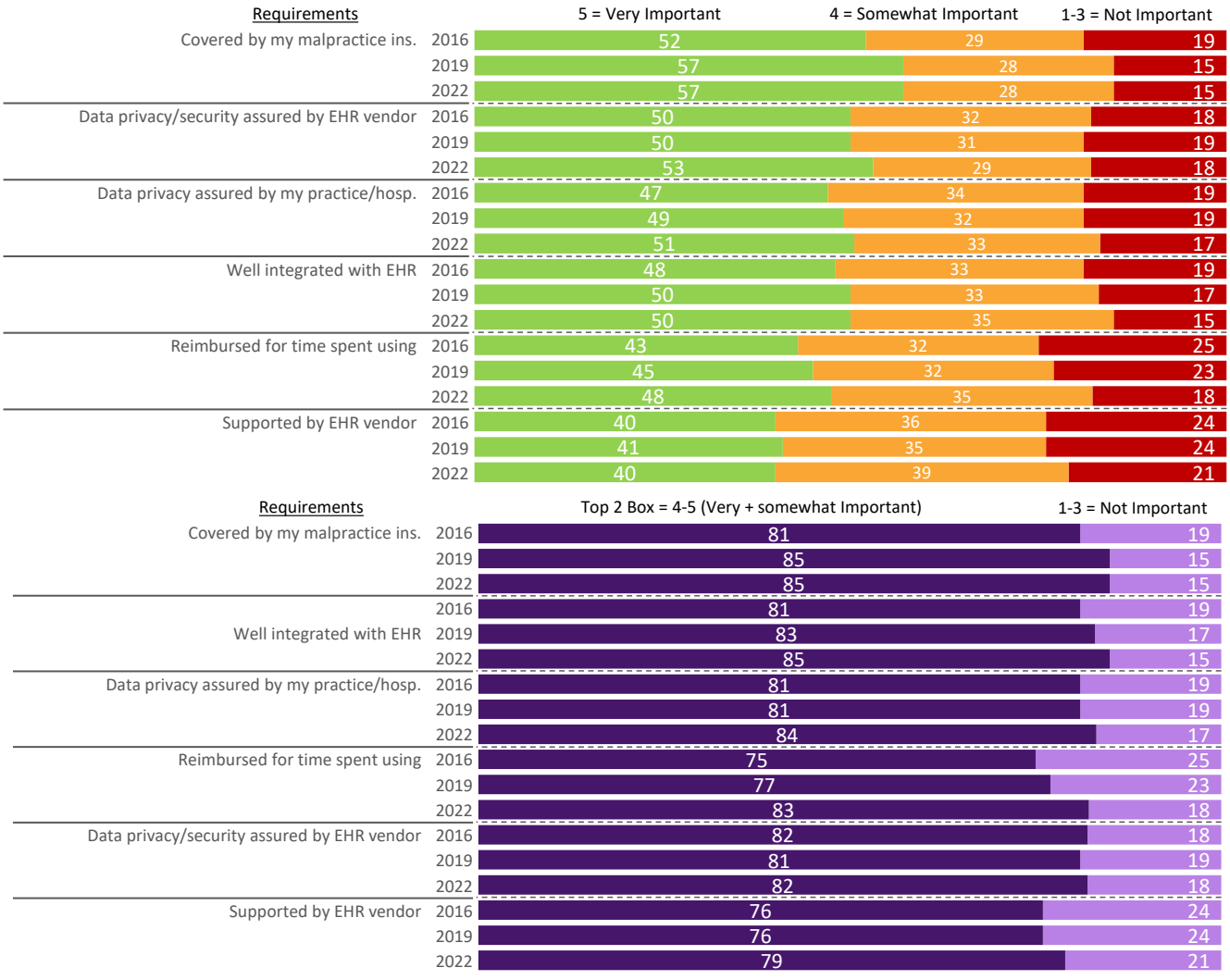
According to the results of the AMA's Digital Health Research report released in September, "covered by my malpractice insurance" is respondents' most common concern, with 85% saying it was either somewhat important or very important to their usage decision. That's more than data security/privacy assurances from the EHR vendor or even reimbursement, both at 82%.

AMA President Jack Resneck, M.D., explains: "If a practice or a system is using a tool to help make care decisions or predict outcomes and the tools ends up being flawed, physicians are concerned that they may end up being unfairly held liable for something that really is an issue with the AI [artificial intelligence] tool."

This concern may especially impact physicians' use of the most advanced technologies. The segment of surveyed providers who are working with such tools remains small, but it is growing.

Around one-fifth of respondents said their practice incorporates "augmented intelligence," a concept of advanced technology "that focuses on AI's assistive role" for practice efficiencies (adopted by 18%) and clinical applications (adopted by 16%). This is a meaningful increase from the 2020 reading, which saw 11% and 6% of respondents, respectively, using these tools. Between 11% and 13% are using biometrics authentication, precision and personalized medicine, and digital therapeutics.

Blockchain as a medical practice tool remains low-use, with a 3% adoption rate – *Roy Edroso (redroso@decisionhealth.com)*



Source: AMA 2022 Digital Health Research report: www.ama-assn.org/system/files/ama-digital-health-study.pdf. Image used with permission.

(continued from p. 4)

"I strongly recommend that if a CE/BA is looking to select a tool, they should try to see if a demo of a tool is available or check with those within their professional networks to see if anyone has recommendations on a tool that they found effective," he adds. "Often, getting input from someone who has actually used a tool and gained hands-on experience with a tool can be a valuable resource in learning about a particular tool."

OCR includes compliance tips in SRA Tool

As another plus, the SRA Tool also includes a wealth of compliance tips for security leaders. Here are some samples:

- Consider reviewing and updating your security risk assessment periodically. Document requirements to update your risk assessment. You may also conduct vulnerability scans. An accurate and thorough security risk assessment should be reviewed and updated periodically or in response to operational changes or security incidents.
- Develop a comprehensive security risk assessment to include all information systems that contain, process or transmit ePHI. Maintain a complete and accurate inventory of the IT assets in your organization to facilitate the implementation of optimal security controls. This inventory can be conducted and maintained using a well-designed spreadsheet.
- Establish a data classification policy that categorizes data as, for example, sensitive, internal use or public use. Identify the types of records relevant to each category. Organizational policies should address all user interactions with sensitive data and reinforce the consequences of lost or compromised data.
- Develop corrective action plans as needed to mitigate identified security deficiencies according to which threats and vulnerabilities are most severe. IT asset management is critical to maintaining the appropriate cyber hygiene controls across all assets in your organization, including medical device management.
- Document threats and vulnerabilities and apply impact and likelihood ratings. This will help determine severity and is the best way to safeguard and protect ePHI from potential threats and vulnerabilities.
- Risks should be formally deemed "accepted" only when appropriate. Conduct routine patching of security flaws in servers, applications (including web applications), and third-party software. Maintain software at least monthly, implementing patches distributed by the vendor community, if patching is not automatic.
- Communicate written results of your security risk analysis to the personnel responsible for responding to identified threats and vulnerabilities. Also consider involving these personnel in the creation of corrective action plans.
- Document policies and procedures to ensure you consistently make informed decisions on the effective monitoring, identification and mitigation of risks to ePHI. Establishing and implementing cybersecurity policies, procedures, and processes is one of the most effective means of preventing cyberattacks.
- Consider all natural and manmade disasters that could affect the confidentiality, integrity, and availability of ePHI. Document how you would respond in these situations to maintain the security of ePHI in your policies and procedures.

Password, authentication tips

On a related note, Avani Desai, CISSP, CISA, CIA, CSA, CCSK, CIPP, PMP, CEO of Schellman, a global cybersecurity assessor, offers the following tips for locking up security in your organizations:

- **Require strong password management**. Per the HIPAA safeguards, password management requirements are quite open-ended, with the safeguard simply requiring the implementation of procedures for creating, changing and safeguarding passwords.

"To properly determine sufficiency for password protection," Desai says, "organizations should perform risk assessments for the systems or services that utilize or house ePHI. While HIPAA itself does not have minimally defined requirements, the risk assessment could be paired with password or authentication requirements from standards such as NIST, PCI or HITRUST to help address the HIPAA safeguard and also define what would serve as optimal for the organization."

Have a question? Ask *PBN*

Do you have a conundrum, a challenge or a question you can't find a clear-cut answer for? Send your query to the *Part B News* editorial team, and we'll get to work for you. Email askpbn@decisionhealth.com with your coding, compliance, billing, legal or other hard-to-crack questions and we'll provide an answer. Plus, your Q&A may appear in the pages of the publication.

- **Go for two-factor authentication**. Two-factor authentication is not explicitly stated as necessary to address HIPAA safeguards. However, organizations should consider two-factor authentication for systems that contain ePHI due to the inherent risks associated with inappropriate access to data or medical records that store this information, Desai says.

"If an organization is considering the pursuit of HITRUST to address HIPAA compliance, then two-factor authentication may become necessary as a HITRUST requirement," Desai says. "A common mistake by organizations is simply not assessing the true or accurate level of risk associated with systems that house ePHI. Based on what the organization defines as their risk level associated with accessing ePHI, they may find that they have either created insufficient password access or parameters to protect their data or, to a lesser degree, that they have implemented excessive layers of authentication and password parameters that create unnecessary costs for the organization." — *Dom Nicastro* (*pbnfeedback@decisionhealth.com*) ■

RESOURCES

- HealthIT.gov, Security Risk Assessment Tool: www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
- Security Rule Guidance Material: www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Coding

CPT Assistant says no to mixing table of risk examples, CPT E/M guidelines

When you train staff on the next update to level-based E/M services, remind them that they can't play mix-and-match with the new guidelines and the 1995 or 1997 Documentation Guidelines for Evaluation and Management Services.

This may come up when your training tackles the examples for the risk of complications and/or morbidity or mortality of patient management category in the updated CPT medical decision-making (MDM) guidelines.

The CPT guideline's examples are based on, but not identical to, the examples in the management options selected column of the 1995 and 1997 guidelines' tables of risk. After the AMA released the new CPT guidelines for office and other outpatient E/M visits (**99202-99215**), some coders and educators wondered if they could still use table of risk examples to code the visits. The CPT Editorial Panel replied with a firm "no" to a question on that topic.

In CPT Assistant, Feb. 2021, the panel explained that even though the information may look the same, there are several differences between the new MDM-based coding method and the 1995 and 1997 guidelines methods.

"MDM in 2021 focuses on the complexity of physician work performed, rather than counting elements," the article states.

In addition, the category definitions aren't the same. The 1995 and 1997 guidelines define risk as "the risk of significant complications, morbidity and/or mortality." The CPT update changed it to "risk of complications and/or morbidity or mortality of patient management," to clarify that MDM documentation — and coding — should be based on "the medically relevant issues for the patient at that specific encounter."

Remind staff that they should not use the 1995 or 1997 guidelines to code E/M claims with dates of service on or after Jan. 1, 2023. However, you can't forget the guidelines. They will need them to perform internal reviews, appeal denials and defend against negative audits of claims submitted on earlier dates. — *Julia Kyles, CPC* (*jkyles@decisionhealth.com*) ■

RESOURCE

- CPT Assistant, Feb. 2021

Correct Coding Initiative

Quarterly edits bring in new bundled services, billing caps

You'll find several hundred new code pairs added to the auto-bundling series of National Correct Coding Initiative (NCCI) edits. The billing updates, which include medically unlikely edit (MUE) additions and revisions, take effect Oct. 1.

The NCCI version 28.3 edits encompass 563 new code pairs and 268 deleted code pairs. The bulk of the added code pairs involve cardiovascular services that make up the 30000 series of the CPT code book. The latest quarterly edits appear to be CCI catching up with billing patterns that have emerged with new codes that were introduced at the beginning of 2022.

For instance, numerous code pair additions in the 30000 series involve procedural codes **33267-33269**, all

of which debuted Jan. 1, 2022. By and large, the new codes pairs take "0" modifier, which means the distinct services are not eligible for same-day billing.

The NCCI program installs automatic edits within claims processing systems to prevent providers from reporting two services together on the same claim when CMS deems them inappropriate. As the NCCI website explains: "Each edit has a Column One and Column Two HCPCS/CPT code. If a provider reports the two codes of an edit pair for the same beneficiary on the same date of service, the Column One code is eligible for payment, but the Column Two code is denied unless a clinically appropriate NCCI PTP-associated modifier is also reported."

The deleted codes pairs taking effect Oct. 1 primarily involve pathology and laboratory services, and nearly all of them involve a code — **U151U** — that was deleted at the start of 2022.

The version 28.3 edits also tag an MUE value on 50 services, ranging from COVID-19 vaccine codes (**91310-91311**) to a brief series of injection codes. An MUE value limits the number of times per day you're eligible to report a unit of service (UOS) for a single patient. The COVID-19 vaccines, for example, will take an MUE of "1".

You will also find more than two dozen services with revised MUE values. For instance, anesthetic injection code **64421** (Injection[s], anesthetic agent[s] and/or steroid; intercostal nerve, each additional level) will see an increase in MUE level from three to four units of service on Oct. 1. There is no change to the code's MUE adjudication indicator (MAI) of 3, therefore practices can appeal denials of additional units. However, the documentation will need to convince a reviewer that the extra blocks were medically necessary.

The update reduced the MUEs for the codes for blocks of genicular nerves and nerves innervating the sacroiliac joint (**64451** and **64454**) and denervation of those nerves (**64624** and **64625**) from two to one. The codes will retain their MAI of 2, which means you will not be able to appeal UOS denials. To avoid denials for bilateral services, report the procedure as one UOS with bilateral modifier **50**. — *Richard Scott* (*rscott@decisionhealth.com*) ■

RESOURCES

- National Correct Coding Initiative: www.cms.gov/medicare-medicaid-coordination/national-correct-coding-initiative-ncci
- NCCI quarterly edits: www.cms.gov/medicare-medicaid-coordination/national-correct-coding-initiative-ncci/ncci-medicare/medicare-ncci-procedure-procedure-ptp-edits

CCI version 28.3 scorecard

Changes effective Oct. 1, 2022.

(For more on CCI version 28.3 edits, see related story, p. 7.)

Code range	CCI code pairs added	CCI code pairs deleted	MUEs added	MUEs deleted	MUEs revised
00000 – 09999	0	0	0	0	0
10000 – 19999	0	0	0	0	0
20000 – 29999	9	1	0	0	2
30000 – 39999	304	0	0	0	2
40000 – 49999	1	0	0	0	0
50000 – 59999	51	0	0	0	0
60000 – 69999	2	1	0	0	8
70000 – 79999	8	0	0	0	0
80000 – 89999	129	191	0	0	6
0001U – 0284U	12	73	36	2	1
90000 – 99999	2	1	2	0	0
0001T – 0999T	5	0	0	0	4
A0000 – V9999	40	1	12	1	4
Totals	**563**	**268**	**50**	**3**	**27**

Note: Code range is based on the comprehensive code of the edit.

Source: Part B News *analysis of CCI version 28.3 changes, www.cms.gov/medicare-medicaid-coordination/national-correct-coding-initiative-ncci/ncci-medicare/medicare-ncci-procedure-procedure-ptp-edits*