June 24, 2024 | Volume 38, Issue 25

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

In this issue

decisionhealth®
an hcpro brand

Billing

Check your telehealth compliance, align POS codes to avoid costly denials

Double check Medicare's telehealth services list before you use a telehealth place of service (POS) code on a claim — or risk an automatic denial. A recent change request from CMS serves as a reminder to make sure you're complying with Medicare's current telehealth requirements.

The COVID-19 public health emergency (PHE) waivers for telehealth services are currently set to expire on Dec. 31, 2024. But effective Jan. 1, 2024, Medicare instructed all providers to report telehealth services with one of the following POS codes based on whether the patient was at home or in another location when they received the telehealth service:

- **02** (Telehealth provided other than in patient's home. The location where health services and health related services are provided or received, through telecommunication technology. Patient is not located in their home when receiving health services or health related services through telecommunication technology.)
- **10** (Telehealth provided in patient's home. The location where health services and health related services are provided or received, through telecommunication technology. Patient is located in their home [which is a location other than a hospital or other facility where the patient receives care in a private residence] when receiving health services or health related services through telecommunication technology.)

Mark your calendar: Virtual summit

The **2024 Billing & Compliance Virtual Summit** provides best practices and proven strategies for building and maintaining a billing and compliance program designed specifically for your practice. Learn from expert speakers as they provide key 2025 payment, CPT and compliance updates, as well as insights into revenue cycle and billing opportunities that will allow you to tap into Medicare's emerging service lines. Learn more: *www.codingbooks.com/billing-compliance-virtual*.

The 2024-effective guidance was a change from the PHE waiver guideline to report the POS for the setting where the in-person visit would have occurred. For example, practices reported POS **11** (Office) if the in-person visit would have taken place in the medical office.

CMS 100-04, Change Request 13582 reminds providers to use the telehealth POS codes and that POS codes 02 and 10 can only be reported with the 268 designated telehealth services. If you report the POS code for a service that isn't on the list, your Medicare administrative contractor (MAC) will deny your claim with group code (GC) **CO** (Contractual obligation), claim adjustment reason code (CARC) **96** (Non-covered charge[s]) and remittance advice remark code (RARC) **N776** (This service is not a covered Telehealth service). You'll have to start the appeals process if you want to get paid.

Because the new rule directly affects reimbursement, make sure your providers are confirming and documenting the patient's location to prevent improper payments. Your practice will receive the facility rate for services you bill with POS 02 and the higher non-facility rate when you report services with POS 10.

Providers must also document the type of connection they used for the telehealth service. The change request clarifies that you should pair the telehealth code with the modifier that shows the type of telehealth connection. For audio-only encounters, report modifier **93** (Synchronous telemedicine service rendered via telephone or other real-time interactive audio-only telecommunications system). For audio and video encounters, use modifier **95** (Synchronous telemedicine service rendered via a real-time interactive audio and video telecommunications system).

"Use of audio-only (93) or audio-video (95) does not change rate of payment, only the POS code determines the non-facility or facility payment rate," CMS explains in the change request. — *Julia Kyles, CPC* (*julia.kyles@decisionhealth.com*) ■

RESOURCES

- CMS 100-04, Change Request 13582: *www.cms.gov/files/document/r12671cp.pdf*
- Medicare telehealth list: *www.cms.gov/medicare/coverage/telehealth/list-services* (Zip file)

decisionhealth®

SUBSCRIBER INFORMATION

Have questions on a story? Call or email us.

***PART B NEWS* TEAM**

Maria Tsigas, x6023
Product Director
maria.tsigas@hcpro.com

Marci Geipe, x6022
Senior Manager, Product and Content
marci.geipe@hcpro.com

Richard Scott
Content Manager
richard.scott@hcpro.com

Roy Edroso, x6031
Editor
roy.edroso@hcpro.com

Julia Kyles, CPC, x6015
Editor
julia.kyles@hcpro.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: *customerservice@hcpro.com*

DECISIONHEALTH PLEDGE OF INDEPENDENCE:
At DecisionHealth, the only person we work for is 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. Every reasonable effort has been made to ensure the accuracy of the information contained herein. However, the ultimate responsibility for correct billing and compliance lies with the provider of services. DecisionHealth, its employees, agents and staff make no representation, warranty or guarantee that use of the content herein ensures payment or will prevent disputes with Medicare or other third-party payers, and will not bear responsibility or liability for the results or consequences resulting from the use of the content found herein.

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, a division of HCPro LLC. *Part B News* is published 48 times/year by DecisionHealth, 35 W. Wacker Drive, 16th floor, Chicago, IL 60601-5809.
ISSN 0893-8121. *pbncustomer@decisionhealth.com* Price: $699/year.

Practice management

Forced to close temporarily? Mind your patient, payment responsibilities

If your practice has to temporarily suspend operations for more than a short duration, you may have to approach patients as if the practice were closing for good and provide recommendations for alternative treatment. You may also have to give providers paid on productivity some bad news.

Sometimes a practice will experience a "force majeure" — a fire or lightning strike, the death or disability of a key provider or other emergency — that requires suspension of its live services for days, weeks or even months. If it's only a very short break with a reasonable estimated end date, Christina M. Kuta, an attorney with Roetzel & Andress in Chicago, thinks some extra time spent rescheduling and a live operator to handle calls might cover it.

"If it's going to be shut down for just a couple of days, you'd reach out to the patients who are already scheduled for appointments, let them know they'll have to reschedule and just make sure someone's available to answer the phone," Kuta says. "If no one's in the office, you always can reroute a phone to someone's house or cell phone to make sure that patients' calls can be answered and directed as needed."

Even in this limited-impact circumstance, J. Malcolm DeVoy, a partner with the Holland & Hart firm in Las Vegas, suggests that you offer patients appropriate provider referrals, particularly in cases where "it is uncertain whether the patient could be seen [by a new provider] within a timeframe of one to two days. These alternatives avoid complaints and potential liability."

But if it goes on for more than a few days and patients could suffer significant care interruptions, you should have a longer-term contingency plan ready to go. As the North Carolina Medical Board says with regard to "precipitous" closings, "No physician expects they will find themselves in a position to cease practice without warning, either temporarily or permanently. Developing written policies and procedures beforehand which address this issue will go a long way toward easing a very difficult transition."

Patients first

Unlike customers of other kinds of business, patients require extra attention. State laws and payer contracts vary on specifics and time frames but, in the experience of attorney R. Ryan Morris of the Gunster law firm in Jacksonville, Fla., you retain responsibility for your patients even if you can't have them at the office, and will have to let them know where they can get care if you're not available to provide it to them.

"Your number one priority should be the patients and communications with them," Morris says. "If you're a little one-physician shop you may not have the resources to keep somebody on staff full time to answer the phone … you will want to make sure you've got a voicemail account set up, and somebody returning these calls promptly."

Along with showing your natural solicitude toward patients, this should also insulate you from patient abandonment claims, Morris says. "If you can't service the patient," he adds, "you should be giving them names and addresses and phone numbers and contact information for somebody who can."

Also bear in mind some patients will need more than a temporary fill-in physician: While your referred patient can forward their records and receive appropriate follow-ups elsewhere, some will also have standing prescriptions or labs with you; to ask them and their temporary provider to reinitiate these for a couple of weeks or months before the patient can return to your care may be considered unreasonably cumbersome and an impediment to treatment.

For these reasons, DeVoy thinks you should implement closure-specific policies and procedures as the North Carolina board suggests, and that they should be generous in provision of standby service: The office manager, for example, should be empowered to operate "a skeleton crew" of non-clinical staff and, if possible, coordinate with providers from other practices about picking up patients. "Planning often is the difference between these emergencies being inconvenient or debilitating to a practice and its long-term viability," DeVoy adds.

No office? Go online

Your providers may be able to provide patients some out-of-office care via telehealth, which the

COVID pandemic showed patients adapt to readily when circumstances call for it (*PBN 3/18/24*).

You're in better shape for this if you currently have some telehealth going and understand its technical, legal and regulatory requirements and limits. And practice and patient type matter: Morris notes that E/M visits and simple follow-up appointments for established patients fit the model more easily than, say, evaluations for controlled substance prescriptions. "While many jurisdictions have embraced telehealth and it is now well accommodated in Medicare payment rules, the technology does not lend itself to all practices, such as dermatology or rheumatology," DeVoy says.

Hold the record

Your responsibility as custodian of patient records persists, as it would if you were permanently closed, though in a temporary closure it would probably be inefficient to offload that responsibility as most retiring providers do. If you have an active employee taking calls and emails, this person should also accommodate whatever access requests your patients need help with.

But your HIPAA responsibilities also persist, Kuta warns, and "if you're relying on your office manager to provide records to patients, for example, and she's working from home because the office isn't occupiable, you need to make sure that the office manager's laptop is secure and she still [observes] the security protocols," he says.

If you're one of that vanishing breed that maintains records on paper instead of the cloud, and the disaster precipitating your closure damaged or destroyed those records, you're going to have to answer to the HHS Office for Civil Rights (OCR) for failing to protect them. If that doesn't scare you into an EHR, Kuta suggests you should at least shell out for fireproof file cabinets.

What about payroll?

It's not just your patients who are suffering the outage — so is your staff. Unless you intend to keep them working on the skeleton crew, you may want to decommission them during the break. As many if not most non-clinical positions are at-will, you can probably furlough or lay off those employees for the duration, though a conference with an employment lawyer is recommended. (Be aware these employees can file for unemployment which, in many states, you will help pay.)

Your contracted providers are another matter. Some of them may be on straight salary, in which case you're now paying them to do, essentially, nothing. Some might be paid on productivity, in which case they're the ones losing money.

"We saw issues with this when COVID happened," Kuta recalls. "Pre-COVID, a lot of employment agreements for doctors did not address the shutdown of the practice for a period of time as a reason to terminate. From the practice's perspective, if the office was closed for an extended period, they had to retain physicians at least through the without-cause notice period in their employment agreements."

COVID taught "savvy health care lawyers" to draft agreements that a shutdown is a "termination for cause" reason, usually with a fixed time limit.

Kuta recommends that you prepare for the unlikely, but still possible, scenario of a shutdown. "Maybe once a year run a drill, spend a couple hours figuring out how you would work in an environment where your computers are out or you don't have an office to go to," Kuta says. "Spend time thinking about if something happens that interrupts your normal flow of business, how you would handle that." — *Roy Edroso* (*roy.edroso@decisionhealth.com*) ■

RESOURCE

- North Carolina Medical Board: "The Doctor is Out: A Physician's Guide to Closing a Practice": *www.ncmedboard.org/images/uploads/article_images/Physicians_Guide_to_Closing_a_Practice_92619.pdf*

Patient encounters

While bird flu crossover risk remains low, take easy steps to be ready

You and your patients almost certainly haven't had any contact with bird flu (H5N1), but given recent global and national concerns over the possibility of animal-to-human transmission now is a good time to give your staff a heads-up on it.

You have probably seen H5N1 and its "novel avian influenza A" cousin H7N9 mentioned in news stories about the virus' recent global spread from birds to cattle and to other animals, including cats, along with the unease among public health officials over the

(continued on p. 6)

Benchmark of the week

Providers favored the on-campus setting for outpatient services in 2022

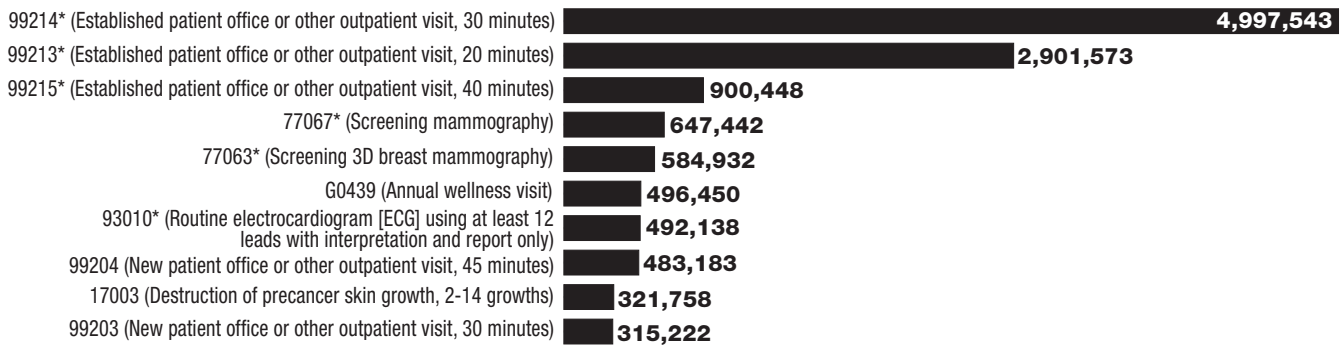
Outpatient services performed on a hospital's main campus dominated the incidence of total outpatient services in 2022, encompassing a far greater share of visits than their off-campus counterparts.

Providers must report outpatient services with place of service **22** (On campus — outpatient hospital) or **19** (Off campus — outpatient hospital). According to the latest available Medicare Part B claims data, 81% of outpatient services were performed in POS 22. The remaining 19% were performed in POS 19.

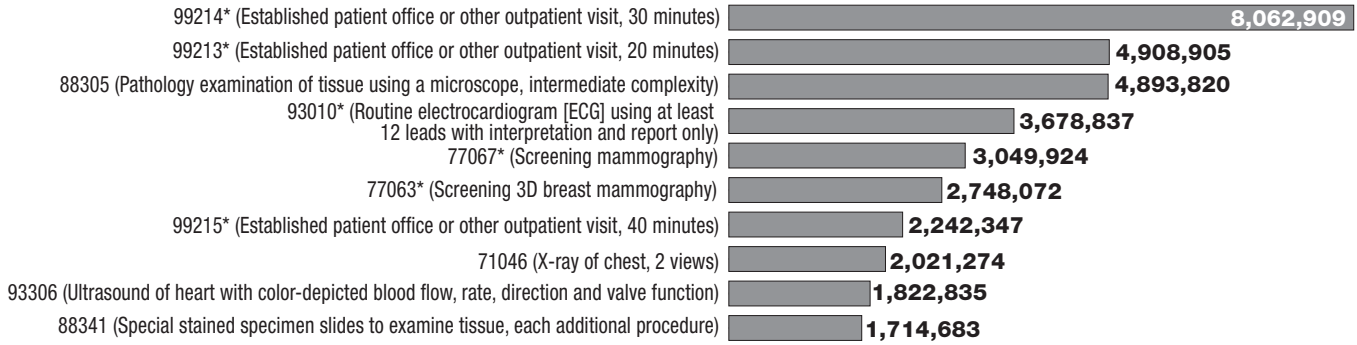
CMS implemented POS 19 in 2016 in response to concerns about improper place of service reporting, including the possibility that providers were reporting services at off-campus, hospital-owned practices with POS 11 (Office) and being paid the higher non-facility rate. Services in POS 19 and 22 are paid at the facility rate.

The following charts show the top 10 services for both settings. Established office or other outpatient E/M visits **99214** and **99213** were the top services in both settings. Four other services, including level five established patient visits (**99215**), screening mammography (**77063, 77067**) and interpretation and report of a routine electrocardiogram with at least 12 leads (**93010**), appeared on both lists. Services that were in the top 10 for both settings are marked with an asterisk (*). — *Julia Kyles, CPC* (julia.kyles@decisionhealth.com)

Top 10 services & procedures in POS 19 – 2022



Top 10 services & procedures in POS 22 – 2022



Source: Part B News *analysis of 2022 Medicare claims data*

(continued from p. 4)

small-but-not-zero possibility of humans catching and spreading the disease.

Since the virus' discovery in 1997, only about 900 humans have caught bird flu worldwide. According to the New York Times, in 2024 15 people in America, China and South America caught it; one of the Chinese sufferers died.

Richard F. Cahill, vice president and associate general counsel of the Doctor's Company in Napa, Calif., notes that recent outbreaks "tend to occur in rural agrarian regions and primarily affect poultry, dairy cattle and wild birds," and the chance of a human epidemic or pandemic are thought to be "marginal."

Nevertheless, Cahill says, you don't want to be caught off guard. The CDC is regularly updating its bird flu guidance for the public and for providers (*see resources, below*). The latter includes a Clinical Overview recommendation for antiviral treatment of "confirmed, probable, or suspected/cases under investigation of novel influenza A virus infection associated with severe human disease" in outpatient settings, as well as isolation, notification of public health departments and other preparatory tasks. CDC also has guidelines on contacting health authorities who can handle related tests.

Cahill says providers should take a cue from previous alert protocols for COVID and for measles (*PBN 4/22/24*):

- Read all published alerts to understand the clinical signs and symptoms as well as the potential risks.
- Proactively implement written protocols to identify possible cases of infection among patients, staff, vendors and other visitors to the practice and to institute procedures to help minimize the spread.

As the COVID pandemic should have inspired you to do, have appropriate personal protective equipment (PPE) ready for handling suspected cases (*PBN 7/27/20*). — *Roy Edroso* (*roy.edroso@decisionhealth.com*) ■

RESOURCES

- New York Times, "A Bird-Flu Pandemic in People? Here's What It Might Look Like," June 17, 2024: *www.nytimes.com/2024/06/17/health/bird-flu-pandemic-humans.html*
- CDC, "Highly Pathogenic Avian Influenza A(H5N1) Virus: Identification of Human Infection and Recommendations for Investigations and Response," April 5, 2024: *https://emergency.cdc.gov/han/2024/han00506.asp*
- CDC, "A(H5N1) Bird Flu Response Update June 14, 2024": *www.cdc.gov/bird-flu/spotlights/h5n1-response-06142024.html*
- CDC, "Clinical Overview of Evaluating and Managing Patients Exposed to Birds Infected with Avian Influenza A Viruses of Public Health Concern," May 3, 2024: *www.cdc.gov/bird-flu/hcp/clinicians-evaluating-patients/?CDC_AAref_Val=https://www.cdc.gov/flu/avianflu/clinicians-evaluating-patients.htm*
- CDC, "Interim Guidance on the Use of Antiviral Medications for Treatment of Human Infections with Novel Influenza A Viruses Associated with Severe Human Disease," May 24, 2024: *www.cdc.gov/bird-flu/hcp/novel-av-treatment-guidance/index.html*
- CDC, "Interim Guidance on Testing and Specimen Collection for Patients with Suspected Infection with Novel Influenza A Viruses with the Potential to Cause Severe Disease in Humans Testing Procedures for Laboratory Personnel," May 8, 2024: *www.cdc.gov/bird-flu/php/severe-potential/?CDC_AAref_Val=https://www.cdc.gov/flu/avianflu/severe-potential.htm*

Ask Part B News

Make sure anticoagulation management visits show medical necessity

Question: *Can we bill **99211** for an anticoagulation monitoring check when the patient does not see the provider during the visit?*

Answer: You may report 99211 when the visit is medically necessary, meets incident-to supervision requirements and the documentation supports a separately billable visit. When there is no separately identifiable E/M visit — for example, the patient just comes in for a routine test — you should not report the visit with 99211.

Several Medicare administrative contractors (MAC) give additional guidance on when you may and may not report 99211 for anticoagulation monitoring visits.

Noridian states that "if the patient presents for … anticoagulation monitoring where there is a documented, medically necessary decision by the physician to change or maintain medication dosage, 99211 may be appropriate. In this case the medical record must document that the history and/or exam required a decision and that the physician made the decision, even though the physician does not personally see the patient."

National Government Services' job aid for 99211 includes a checklist with the following item: "For evaluation of patient anticoagulation status, does the patient have new symptoms or a change in medication dosage?" (*See resources, below.*)

CGS Administrators' article on billing anticoagulation management gives a detailed list of dos and don'ts for reporting a visit with 99211.

For example, make sure providers document the patient's indication for anticoagulant therapy, current dose, prothrombin time and international normalized ratio (INR) results; assess the patient for signs of bleeding or other adverse reactions to anticoagulation therapy; and identify the ancillary staff who performed the visit and the supervising physician.

The list of activities that don't justify a separate E/M visit include repetitive education that isn't customized for the individual patient; the supervising physician is not treating the condition that requires the anticoagulant therapy; or "when the only documentation would be vital signs, the patient's current and future dose of anticoagulant, and when lab work is to be repeated," CGS writes. *— Julia Kyles, CPC (julia.kyles@decisionhealth.com)* ■

RESOURCES

- CGS – Billing 99211 for Anticoagulation Management: www.cgsmedicare.com/partb/cert/articles/015.html
- National Government Services: www.ngsmedicare.com/en/web/ngs/evaluation-and-management?lob=96664&state=97178&rgion=93623&selectedArticleId=3128150
- Noridian — 99211 and Incident To: https://med.noridianmedicare.com/web/jeb/cert-reviews/cert/99211-and-incident-to

Compliance

Be proactive, follow procedures when grappling with cyberattacks

Editor's note: *In this week's issue, Rebecca Herold, CDPSE, FIP, CISSP, CIPM, CIPP/US, CIPT, CISM, CISA, FLMI, HIPAA security and privacy training expert and CEO of Privacy & Security Brainiacs SaaS services, shares best practices when grappling with the fallout of a cyberattack.*

Question: *In the event of a cyberattack, how should health care entities document their response efforts to demonstrate compliance with HIPAA regulations to OCR?*

Answer: Every covered entity (CE) and business associate (BA) must ensure they have detailed procedures to follow when cybersecurity incidents of all types, including cyberattacks, and privacy breaches occur.

Specifically, regarding what needs to be documented, here are key details necessary not only to demonstrate compliance with HIPAA, but also to demonstrate due diligence in the event of an investigation, lawsuit or other type of contentious situation. It is important that documentation is created before any privacy breaches or security incidents, as well as during the response, notice and recovery activities. Keep in mind this is a high-level overview. Determine if additional information is needed based upon the context of each situation.

Before breaches and incidents occur:

- Document roles and responsibilities for security, privacy and HIPAA compliance requirements. These are usually found within the security and privacy policies. Make sure this documentation includes roles for managing breaches/incidents, for communicating with entities outside the organization (e.g., TV and news reporters, lawyers), and for maintaining a chain of custody for associated evidence.
- Document policies and supporting procedures for incident and breach identification, response and recovery. Make sure they are in compliance with the HIPAA Breach Notification Rule and include additional actions as necessary for the organization's digital ecosystem and the context of each breach and incident.
- Establish a reporting mechanism and a process for the organization, and all BAs, to use in the event of a security incident or privacy breach.
- Document the types of training and ongoing awareness communications and activities about the incident and breach policies and procedures. These should also include a log or history of when such training was provided within the last year, and of those attending the training and passing the subsequent exam to confirm understanding.
- Review and document all vendor and contractor relationships to ensure BAAs include details to support appropriate actions they need to take, including documentation and time frames for contacting specified roles within the organizations they are supporting, while also clearly describing all the BA's privacy breach and security incident obligations.

During the breach and incident response:

- Log/document all activities and factors involved with the breach and/or incident. Include dates, times, names, locations, types of data and associated technical, operational, administrative and physical de-

tails. These will be more than are necessary to report to HHS, because they will be needed for the organization to understand why the breach/incident happened to begin with and to determine how to prevent a similar type of event from happening again.

- Ensure specific information necessary to report to HHS is clearly, accurately, and centrally documented by the breach/incident management role. These include the primary contact and associated information at the organization managing the breach and/or whom HHS can contact with any questions; details about any BAs involved; how many individuals' PHI was involved (the exact number, or a good estimate if an exact number is not possible); breach start date; breach end date; discovery start date; discovery end date; type of breach; location/tech type of breach; types of PHI breached; a succinct description of the breach; the safeguards that were in place prior to the breach; and notice of breach and associated actions taken.
- BAs (including subcontractors) must make sure they are documenting these same details to send to their CEs, or BAs, if they are sub-contractors.

During recovery activities:

- Document all vulnerabilities and threats that led to the breach and/or incident and actions that will be taken to prevent similar events from recurring.
- Document and incorporate lessons learned from the events into the overall security management process.
- Update and implement, as necessary, BAAs when events involved exploitation of vulnerabilities and threats against, through, and/or from BAs.
- CEs must complete and submit the required HHS reports within 60 days of the discovery of the breach (for incidents involving 500 or more individuals) or within 60 days of the end of the calendar year in which the breach was discovered (for breaches involving fewer than 500 individuals).
- Perform a documented risk assessment for the scope of applicability for where the breach and/or incident occurred. — *Rebecca Herold, CDPSE, FIP, CISSP, CIPM, CIPP/US, CIPT, CISM, CISA, FLMI* (*pbnfeedback@decisionhealth.com*) ■

Coding

HCPCS codes released for COVID-19 prophylaxis after FDA approval

The Food and Drug Administration (FDA) recently announced an emergency use authorization for Pemgarda, a pre-exposure prophylaxis for COVID-19, leading to the release of HCPCS Level II codes for the drug and its administration.

The drug was designed for individuals who are at least 12 years old, weigh at least 88 pounds, are not currently infected with COVID-19, and have a moderate to severe immunocompromising condition or treatment. The products were created by Invivyd.

The HCPCS Level II codes and their definitions according to updates to CMS' vaccine pricing website, are:

- **Q0224** (Injection, pemivibart, for the pre-exposure prophylaxis only, for certain adults and adolescents [12 years of age and older weighing at least 40 kg] with no known SARS-CoV-2 exposure, and who either have moderate-to-severe immune compromise due to a medical condition or receipt of immunosuppressive medications or treatments, and are unlikely to mount an adequate immune response to COVID-19 vaccination, 4500 mg).
- **M0224** (Intravenous infusion, pemivibart, for the pre-exposure prophylaxis only, for certain adults and adolescents [12 years of age and older weighing at least 40 kg] with no known SARS-CoV-2 exposure, who either have moderate-to-severe immune compromise due to a medical condition or receipt of immunosuppressive medications or treatments, includes infusion and post-administration monitoring).

The two codes became effective March 22. — *Savannah Schmidt* (*savannah.schmidt@hcpro.com*) ■

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.