April 29, 2024 | Volume 38, Issue 18

Part B News

partbnews.com

COLLECT EVERY DOLLAR YOUR PRACTICE DESERVES

In this issue

decisionhealth®
an hcpro brand

Compliance

HHS OCR: Penalize non-compliant employees to protect privacy, security

Make sure your HIPAA compliance toolkit includes a few sticks to punish employees who violate your practice’s compliance guidelines, along with any carrots you use to reward compliance. And warn staff that the practice can’t let violations slide: Sanctions for HIPAA non-compliance are mandatory and the threat of punishment is designed to encourage compliance and safeguard patients, protected health information (PHI) and your practice from a breach.

The HHS Office for Civil Rights (OCR) reminded all covered entities that “the need for constant vigilance to protect [electronic protected health information {ePHI}] is at an all-time high due to hacking and other threats” and that sanctions “are specifically required by both the Privacy Rule and the Security Rule,” in the OCR’s latest cybersecurity newsletter.

For example, the privacy rule states that covered entities and business associates must “have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of [the Privacy Rule] or [the Breach Notification Rule],” and the security rule has a similar provision, the OCR explains in the October 2023 newsletter.

In practical terms, this means that if your internal investigation of a breach reveals that it was caused by an employee who fell for a phishing attack and you don’t sanction the employee, the OCR could say that failing to sanction the employee was a second HIPAA violation.

Use the following highlights to make sure your practice, patients and employees get the most out of your HIPAA compliance sanctions policy.

Scale, share and apply sanctions

Employees who cause a breach at your practice should be sanctioned whether the breach was accidental or intentional. However, HHS allows organizations to design their own policies "in a manner consistent with numerous factors, including such things as, but not limited to, their size, degree of risk, and environment," according to the Health Insurance Reform: Security Standards rule, which was published Feb. 2, 2003.

Make sure the punishment fits the circumstances. The rule suggests that an organization's sanctions be "appropriate to the nature of the violation," and "vary depending on factors such as the severity of the violation, whether the violation was intentional or unintentional, and whether the violation indicated a pattern or practice of improper use or disclosure of protected health information," and range from a warning to termination.

Your policy could require a warning when employees share their login and password with coworkers, extra compliance training for employees who fall for a phishing attempt and automatic firing of employees who post a patient's PHI on social media. Sanctions also should reflect your compliance training. For example, make sure you have trained employees not to share passwords if you create a sanction for password sharing.

Employees should never be surprised by sanctions. Your HIPAA compliance training should spell out the sanctions policy and include examples of behavior that could trigger a sanction. Remember, the purpose of sanctions is to prevent HIPAA violations by warning employees that they'll be punished if they don't follow the rules.

Finally, you should apply sanctions based on the employee's actions, not on their role or title. Therefore, if you require extra HIPAA compliance training for an employee who shares their password with a coworker, you can't excuse a treating provider from the training but require it for a non-medical member of the practice who makes the same mistake. "Indeed, sanctioning workforce members inconsistently can undermine the integrity of a regulated entity's compliance program," the OCR writes in the newsletter.

Document the sanctions

Document any sanctions in the employee's record. The knowledge that a sanction will go down in their permanent record could serve as another deterrent.

Failing to document employee sanctions, or taking too long to do so, can expose your practice to sanctions after a breach. In its October 2023 newsletter, the OCR cited the example of a Texas health system that "failed to document timely the sanctions imposed against members of its workforce who failed to comply with its privacy policies and procedures or the Privacy Rule," after employees, including senior leaders, allegedly

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.

COPYRIGHT WARNING
Copyright violations will be prosecuted. *Part B News* shares 10% of the net proceeds of settlements or jury awards with individuals who provide essential evidence of illegal photocopying or electronic redistribution. To report violations, contact: David Gilmartin at *generalcounsel@ahima.org.*

REPRINTS
To request permission to make photocopy reprints of Part B News articles, call 1-855-CALL-DH1 or email customer service at *customerservice@hcpro.com*. Also ask about our copyright waiver, multiple copy and site license programs by calling the same number.

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.

decisionhealth®

disclosed one patient's PHI to 15 media outlets and on the health system's website.

The health system paid $2.4 million to resolve the issue and had to enter a corrective action plan. — *Julia Kyles, CPC* (*julia.kyles@decisionhealth.com*) ■

RESOURCES

- October 2023 OCR Cybersecurity Newsletter: *www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-october-2023/index.html*
- Health Insurance Reform: Security Standards: *www.federalregister.gov/documents/2003/02/20/03-3877/health-insurance-reform-security-standards*
- Texas health system settles potential HIPAA disclosure violations: *www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/mhhs/index.html*

Ask Part B News

'Administrative' fees for patient messages? Not if it's about treatment.

Question: *I have seen stories in the press about practices charging "administrative fees" for calls, emails and texts from patients. I can't see how this would be allowed by insurers. Can I really charge for this?*

Answer: In recent months stories on this subject have appeared in the mainstream press, including the Washington Post ("Drowning in patient emails, doctors start charging for their replies"), Fox Business ("Some doctor's offices are charging patients for administrative tasks") and Axios ("The Doctor Will Fee You Now"). All cite physician burnout over administrative tasks and portray the charges for remote communications as a way to cope with it (*PBN 1/31/22*).

As these are mass-market rather than medical industry news reports, they aren't specific about what exactly is being billed. But a Jan. 6, 2023, JAMA research letter cited by some of the reports suggests confusion between "administrative fees" and accepted billing practices for e-visits and virtual check-ins.

The JAMA letter refers to an increase in "patient messaging" during the COVID-19 pandemic and finds "an association with a reduction in patient portal messaging (both threads and individual messages) … that may be attributable to awareness of the possibility of being billed."

What the JAMA authors mean is clearly remote medical treatment, as their description of messaging criteria — "asynchronous patient portal messages that require medical decision-making and at least 5 minutes of clinician time over a 7-day period") — connects it with the codes CMS uses for e-visits. Those codes include:

- **99421** (Online digital evaluation and management service, for an established patient, for up to 7 days, cumulative time during the 7 days; 5-10 minutes).
- **99422** (… ; 11-20 minutes).
- **99423** (… ; 21 or more minutes).
- **98970** (Qualified nonphysician health care professional online digital assessment and management, for an established patient, for up to 7 days, cumulative time during the 7 days; 5-10 minutes)
- **98971** (… ; 11-20 minutes).
- **98972** (… ; 21 or more minutes).

The articles also may be referring to what CMS calls virtual check-ins, such as **G2012** (Communication technology-based service by a physician or other qualified health care professional who can report E/M services).

There are few genuinely administrative tasks associated with medical treatment that the law and insurers allow to be billed, and only under certain circumstances. For example, when you provide medical records to patients, normally a free service under HIPAA, you can bill for it in certain extraordinarily labor-intensive cases (*PBN 9/9/19*, *5/22/23*).

But Richard F. Cahill, vice president and associate general counsel of the Doctor's Company in Napa, Calif., says if you try to slip an "administrative" fee into any bill that goes to a payer, it will "undoubtedly be rejected as not medically necessary and will probably be considered as a customary cost of doing business that should not be reimbursed."

Your office might make a case for patient charges that are wholly divorced from medical treatment — for example, parking. By that logic, you might also justify charging them for communications that have nothing to do with their treatment, though it's hard to imagine what such communication would look like. Cahill suggests that a call or text about insurance details, or when the pharmacy will get the prescription discussed in an earlier visit, might qualify. But squabbling over it is likely not worth your while.

Ultimately, you and your patient must be absolutely clear in advance on what non-medical services you expect to be paid for. "Individuals in professional settings dislike surprises," Cahill says.

If there's any kind of add-on non-medical service for which you might charge, make sure it's spelled out in the policies and procedures (under what some practices call a "conditions of treatment agreement") to which the patient must agree when they walk in the door. But e-visits and virtual check-ins are treatment, and you should bill them as such. — *Roy Edroso* (*roy.edroso@decisionhealth.com*) ■

RESOURCE

- JAMA, Research Letter, "Association Between Billing Patient Portal Messages as e-Visits and Patient Messaging Volume," Jan. 6, 2023: *https://jamanetwork.com/journals/jama/fullarticle/2800370*

Ask Part B News

Make sure TPIs scheduled before April 1 will meet new LCD policy

Question: *Our Medicare administrative contractor (MAC) has adopted the new local coverage determination (LCD) for trigger point injections (**20552-20553**). The LCD limits the number of trigger point injections a patient may receive to three sessions per rolling 12-month period.*

Our practice's staff wants to know if the rolling 12-month period begins on April 1, 2024, the effective date for the LCD, or does it include trigger point sessions before April 1?

For example, a patient received trigger point injections on Jan. 11, 2024, and March 3, 2024. The patient is scheduled to receive another injection on April 24, 2024. Will the April 24 visit count as the third injection under the LCD?

Answer: No. The LCD does not apply to services the patient received before the LCD went into effect. The April 24 trigger point injection might count as the first of three allowed services and the 12-month calendar would begin on that visit.

However, the April 24 trigger point session must meet the new LCD's requirements, even though it was scheduled before the policy went into effect (*PBN 3/25/24*). For example, if the patient is not being treated for a tension-type headache (**G44.201-G44.229**) or myalgia (**M79.10-M79.18**), your MAC will not cover the service. — *Julia Kyles, CPC* (*julia.kyles@decisionhealth.com*) ■

RESOURCE

- Trigger point injections, LCD L39662 — National Government Services: *www.cms.gov/medicare-coverage-database/view/lcd.aspx?lcdid=39662&ver=5&lcdStatus=all&sortBy=title&bc=6*

Benchmark of the week

Virtual check-in, e-visit codes opened strong in 2020, then collapsed

There was a burst of enthusiasm among providers when e-visits became billable to Medicare at the outset of the COVID-19 pandemic, but that excitement quickly waned and hasn't bounced back.

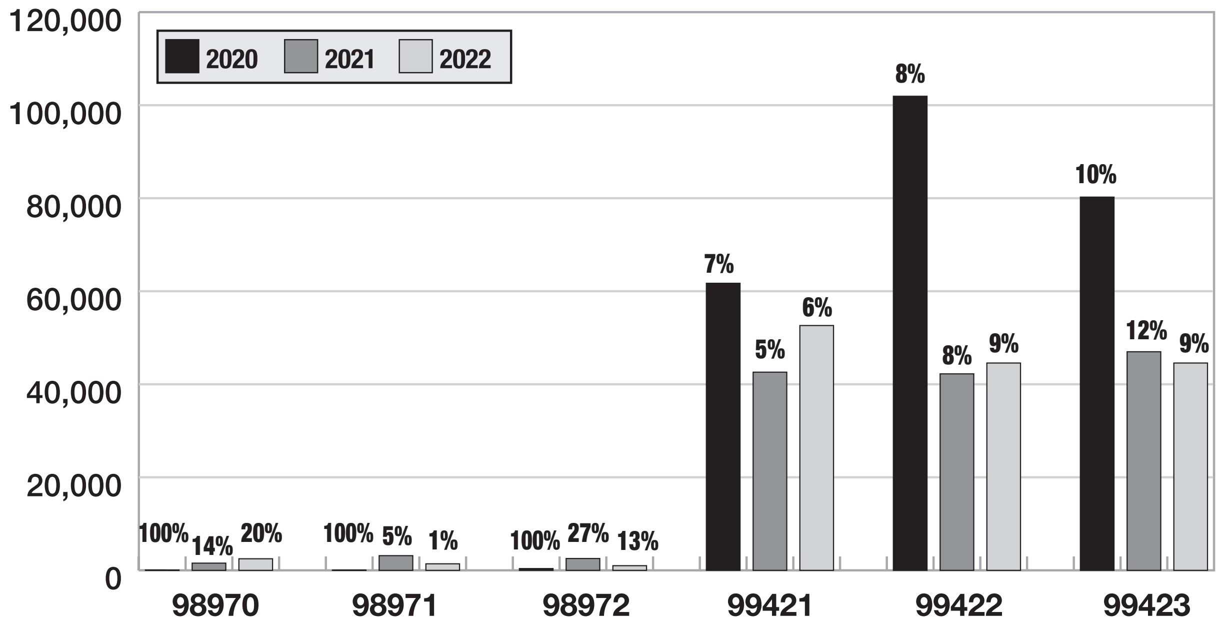
The initiation at the outset of 2020 of six e-visit codes for "online digital evaluation and management service" in the case of physicians, and "digital assessment and management" for non-physician practitioners was fortuitous (*PBN 1/13/2020*). When the pandemic kicked in a few months later, it gave providers a new, germ-free way to deal with COVID-panicked patients, especially when the physician codes (**98970-98972**) were cleared for new as well as established patients (*PBN 5/18/20*). While the codes for non-physician practitioner (NPP) treatment (**99421-99423**) started slowly — and have mainly stayed slow — the three physician codes together garnered more than 244,000 claims in 2020.

But as you can see from the chart below, there was a utilization collapse in 2021 and the three physician codes fell to about 132,000 claims, a drop of 46%. This was despite the decent denial rates the codes earned. The NPP codes started out with little interest, perhaps due to some last-minute changes in their description and scope (*PBN blog 3/2/20*). Several of the codes, including 98970, 99421 and 99422, inched up a bit in 2022, according to the latest available Medicare claims data, but the others still continued their descent.

A similar tale of woe bedevils the "virtual check-in" codes for forwarded digital data, not pictured in this chart: While **G2012** (Communication technology-based service by a physician or other qualified health care professional who can report E/M services) began with a spectacular 847,525 claims in 2020 (and a 6% denial rate), it collapsed in two years to 122,219 claims, an 86% drop. The other two codes (**G2251-G2252**) have never gotten out of the low thousands.

The lion's share of these codes have been claimed by primary care providers (internal medicine, family practice and nurse practitioner specialties), though cardiologists reported 8,242 claims for G2012 and 2,950 claims for 99243 in 2022. — *Roy Edroso* (*roy.edroso@decisionhealth.com*)

Medicare e-visit code utilization, 2020-2022, with denial rates



Source: Part B News *analysis of 2020-2022 Medicare claims data*

Compliance

Take tips from Green Ridge cybersecurity case to bolster compliance

In a significant development underscoring the growing threat of cyberattacks in the health care sector, the Office for Civil Rights (OCR) recently announced a settlement with Green Ridge Behavioral Health LLC concerning a ransomware attack that compromised the protected health information (PHI) of over 14,000 individuals.

This incident serves as a critical reminder of the importance of HIPAA compliance and the need for robust cybersecurity measures to protect sensitive health information.

Rising cyberthreats, prevention steps

Here's what you need to know about this settlement and ransomware attack:

- **Ransomware attack on Green Ridge Behavioral Health:** The settlement follows an investigation into a ransomware attack that encrypted the electronic health records (EHR) of all patients at Green Ridge Behavioral Health, a Maryland-based psychiatric practice.
- **HIPAA violations and settlement terms:** The OCR's investigation identified potential violations of the HIPAA Privacy and Security rules, including failures in risk analysis, implementing security measures, and monitoring health information systems. As part of the settlement, Green Ridge Behavioral Health has agreed to pay $40,000 and engage in a corrective action plan monitored by OCR for three years.
- **Corrective action plan:** The plan includes conducting a thorough risk analysis, designing a risk management plan, revising policies and procedures, conducting workforce training on HIPAA policies, auditing third-party arrangements, and reporting noncompliance instances.
- **Rising cyberthreats in health care:** OCR highlights a significant increase in hacking and ransomware incidents in health care, with hacking accounting for 79% of the large breaches reported in 2023. These breaches have dramatically impacted the privacy and security of millions of individuals' health information.
- **Recommended best practices for HIPAA compliance:** OCR recommends several best practices to mitigate cyberthreats, including regular risk analyses, ensuring business associate agreements (BAA), implementing audit controls, utilizing multifactor authentication (MFA), encrypting PHI, incorporating lessons from incidents, and providing targeted training.

The recent settlement between OCR and Green Ridge Behavioral Health serves as a stark reminder of the vulnerabilities within the health care sector to cyberattacks such as ransomware. It also emphasizes the critical importance of HIPAA compliance officers in ensuring that health care providers, health plans, clearing-houses and their business associates strictly adhere to the HIPAA Privacy and Security rules in order to protect patient information.

Through diligent risk management, implementing strong security measures and fostering a culture of compliance and awareness, organizations can safeguard against the increasing threat of cyberattacks. This incident not only highlights the need for ongoing vigilance but provides valuable insights into the strategies that can be employed to enhance the security and privacy of health information.

Q&A on ransomware breach

In this issue, Liz Heddleston, a principal in the Health Law and Cybersecurity & Data Privacy practices at Woods Rogers Vandeventer Black in Virginia, discusses the breach and provides medical groups with action steps for prevention and compliance.

How can health care organizations better prepare for the increasing threat of ransomware?

Heddleston: Health care organizations juggle competing priorities but, given the increasing threat of ransomware, cybersecurity needs to be top of mind for leaders. Bottom line: It's a matter of patient safety. Ransomware attacks can disrupt operations and interfere with patient care. Maintaining a strong cybersecurity and HIPAA compliance program can help prevent ransomware attacks, but it takes a significant financial commitment and resources. There needs to be buy-in from across the health care organization.

The Department of Health and Human Services (HHS) recently released cybersecurity performance goals, which can help health care organizations prioritize the most effective safeguards for protecting patient data. They include measures such as strong encryption and MFA. The HHS goals are voluntary for now, but the agency plans to pass regulations that make them mandatory. Health care organizations also need to ensure their HIPAA compliance program is effective and current.

What role does employee training play in preventing cybersecurity breaches, and what are the best practices for implementing this training?

Heddleston: Don't underestimate the role that employees play in helping to prevent ransomware attacks. The vast majority of ransomware attacks begin with phishing. Employees are truly on the front lines when it comes to preventing cyberattacks. Phishing emails can be very convincing at imitating legitimate emails, and they exploit the fact that so many of us receive a high volume of emails and are pulled in many directions, putting us more at risk for missing the warning signs of phishing.

Cybersecurity training should be more than just a check-the-box exercise that happens once a year. It needs to be delivered continuously through multiple channels, such as by email, videos, posters and signs. The training needs to be regularly updated to address the evolving nature of threats and new tactics used by hackers. Simulated phishing exercises, such as sending mock phishing emails to employees, are a great training tool.

Don't underestimate the role that employees play in helping to prevent ransomware attacks. The vast majority of ransomware attacks begin with phishing.

Can you explain the importance of conducting regular risk analyses and how they should be integrated into the health care organization's ongoing operations?

Heddleston: Risk analyses are the backbone of any effective HIPAA compliance program and can play an essential role in preventing cyberattacks. They are designed to help an organization identify the risks and vulnerabilities to electronic PHI that exist across an organization. On a basic level, a health care organization cannot effectively protect its patient data unless it fully understands where its PHI exists and how it is shared inside and outside the organization.

A good risk analysis includes input from across the organization, from the IT team to the clinical team. Health care organizations should complete risk analysis annually, at a minimum, and after a significant security incident or any significant change to the IT infrastructure or operations, such as the implementation of a new EHR.

What are the key components of a robust risk management plan for health care organizations to withstand cyberattacks?

Heddleston: Once an organization has identified the major threats to its patient data through risk assessment, it needs to come up with a plan of attack. A list of pie-in-the-sky goals — without follow-through and accountability — will not cut it. A good risk management plan includes concrete steps to mitigate the most significant threats to patient data. The plan must hold the health care organization accountable for its commitments. Each remediation measure should include a timeline for implementation and a person or group in charge of seeing it through. The health care organization needs to track and document its progress with the risk management plan and adjust as necessary.

How should health care organizations approach third-party vendor management to ensure HIPAA compliance and minimize breach risks?

Heddleston: Health care organizations need to have a good handle on who is handling their sensitive patient data inside and outside the organization. Health care organizations must identify and track all third-party vendors who handle patient data and ensure they have a BAA with each vendor.

Health care organizations should perform due diligence on their vendors to ensure they have sufficient measures to protect patient data and comply with HIPAA. A robust BAA can provide extra legal protections to health care organizations and spur important conversations about a vendor's security infrastructure. Ideally, these conversations must happen at the onset of the relationship, before the contracts are signed, and before vendors are entrusted with patient data. Health care organizations often do not vet their vendors until there is a problem and, by that point, it may be too late.

In the event of a breach, what immediate actions should a HIPAA security compliance officer take to mitigate damage?

Heddleston: The HIPAA security officer needs to escalate the issue to senior leadership immediately. Time is of the essence during a cyberattack. The cyber-insurance carrier also needs to be notified immediately, and the legal team and technical experts need to be deployed as soon as possible. A sophisticated ransomware attack will typically require outside experts who specialize in responding to cyberattacks and will collaborate to ensure a swift and effective response.

How does MFA contribute to the security of PHI, and what challenges might organizations face in implementing it?

Heddleston: MFA makes it harder for hackers to get into your systems by providing extra layers of identity verification. Passwords offer limited protection. Many people reuse passwords across accounts, and passwords are easily compromised. By implementing MFA, you add one or two extra layers of security, making it harder for hackers to get into your systems and steal sensitive data.

Cost can hinder the implementation of MFA, especially for smaller health care organizations. User resistance can also be a challenge. Some employees will view the extra steps required to log in as slow and inconvenient, especially in a fast-paced health care environment.

After a cybersecurity incident, how can health care organizations effectively incorporate lessons learned into their security management processes?

Heddleston: Cybersecurity incidents can be very stressful. Leaders must make quick decisions and are pressured by notification deadlines and legal requirements. When the dust settles, health care organizations must step back and take stock of the incident. Instead of just returning to business as usual after a breach, the organization needs to complete a security risk assessment documenting the vulnerabilities that contributed to the breach. The organization also needs to develop a concrete plan for addressing those vulnerabilities. Accountability is key. The organization needs to make sure the plan doesn't just live on paper — it needs to be implemented to make the organization more resilient in the future.

What are the legal and financial implications of a HIPAA breach due to ransomware for health care organizations?

Heddleston: Ransomware attacks can lead to legal risks and reputational harm and can be costly to contain and remediate. A good cyberinsurance policy is paramount for protecting your organization against these risks. Ransomware attacks impacting PHI need to be reported to HHS-OCR and may trigger an investigation by federal regulators. These investigations can be very detailed and can get into the weeds of what measures you did (and did not) have in place before the breach. Failure to comply with HIPAA can lead to the imposition of corrective action and even fines and penalties in severe cases. Even though the health care organization was the victim of a criminal ransomware activity, it doesn't let you off the hook in terms of HIPAA compliance. — *Dom Nicastro* (*pbnfeedback@decisionhealth.com*) ■

Coding

Take note of new code, billing method for injectable steroid

Make sure your orthopedic practice is up to date on coding for injected methylprednisolone acetate (steroid). Effective for date of service April 1, codes **J1020**, **J1030** and **J1040** are no longer active. Instead, practices should use a new code, **J1010** (Injection, methylprednisolone acetate, 1 mg).

The change means that you will need to report one unit of code J1010 per milligram, so for example if 35 milligrams are injected, you should report J1010 x35 units. Both physician offices and facilities are impacted by the change.

Practices also should double check that the NDC codes they had previously billed with codes J1020 (20 mg), J1030 (30 mg) and J1040 (80 mg) are now aligned with code J1010, suggests coding consultant Bobbi Buell at onPoint Oncology Inc. in San Francisco. — *Laura Evans, CPC* (*laura.evans@decisionhealth.com*) ■

RESOURCES

- HCPCS Quarterly Updates for April 2024: *www.cms.gov/medicare/coding-billing/healthcare-common-procedure-system/quarterly-update*
- April 2024 Update of the Hospital Outpatient Prospective Payment System (OPPS) (Transmittal 12552, March 21, 2024): *www.cms.gov/files/document/mm13568-hospital-outpatient-prospective-payment-system-april-2024-update.pdf*
- Quarterly Update to the Medicare Physician Fee Schedule Database — April 2024 Update: *www.cms.gov/files/document/r12501cp.pdf*