May 15, 2023 | Volume 37, Issue 20

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

In this issue

decisionhealth
an hcpro brand

Practice management

Vaccine mandate slated to end; prepare for pullbacks, challenges in personnel

The White House hints that the COVID vaccination mandates for CMS-affiliated health care facilities will soon come to an end. If this removes your legal obligation to have vaccinated staff (note: it may not), make sure you're ready to make personnel changes in keeping with the new order; if you plan to keep the mandate anyway, prepare for possible challenges.

On May 1 the White House announced that the end of the previously announced COVID public health emergency (PHE) also would mean the end of its vaccination mandates "for federal employees, federal contractors, and international air travelers." At the same time, the administration said it would "start the process" to end vaccination requirements for other entities, including "CMS-certified health care facilities."

The CMS mandate was instituted Nov, 5, 2021, and survived a long series of legal challenges ending with the Supreme Court declining to intervene on Jan. 13, 2022 (*PBN 11/22/21*, *1/17/22*). Since then, most facilities that take CMS payments have been required to make sure staff and contractors with patient contact are vaccinated against COVID. Physician practices are not specifically included, but when they interface with patients in covered entities — as physicians with hospital privileges do — they must also be vaccinated (*PBN 6/6/22*).

Experts agree that the administration will follow through on revoking the CMS mandate, and sooner rather than later.

Sandra M. DiVarco, a partner with McDermott Will & Emery in Chicago, says she's "watching daily because our covered facility clients, much as they had challenges in getting the mandate up and

Prepare for prior auth for facet joints

Effective July 1, 2023, you'll need a prior authorization for facet joint interventions (64490-64495 and 64633-64636) performed in the outpatient setting. And that's not the only risk to your facet claims. The HHS Office of Inspector General (OIG) checked on compliance with the new uniform local coverage determination (LCD) and found significant problems. Ward off challenges by tuning into the live webinar **Facet Joint Interventions: Prepare for Prior Authorizations and More Medicare Audits** on June 6. Learn more: *www.codingbooks.com/ympda060623*.

running in their organizations, are now going to have to understand how to peel it back — and whether CMS will do that in some sort of stepwise manner, or with additional guardrails, hasn't yet been shared."

You can still mandate

But note: Ending the mandate is not the same thing as telling medical organizations that they cannot or should not require staff vaccinations.

"While the mandate's expiration is imminent, each health care facility should still consider, on an organization-by-organization basis, whether it still makes sense to maintain such a requirement," says Ian Schaefer, a labor and employment partner at the Sheppard Mullin firm in New York. While other kinds of businesses are rapidly pulling back their masking, vaccination and social distancing requirements, "health care facilities are clearly different and their services reach the most vulnerable in our population," Schaefer adds.

Paul F. Schmeltzer, a health care attorney with Clark Hill in Los Angeles, advises that providers "conduct an individualized analysis to determine their needs and the associated risks. They should also review their existing policies and practices around vaccination requirements."

Even if you want to pull back, you might have other laws and regulations to consider. Brenda Baumgart, practice group leader for Stoel Rives' labor and employment group in Portland, Ore., notes that "in some jurisdictions ... there is a separate state COVID-19 vaccine mandate for healthcare workers." Oregon, for example, rolled out one such mandate before the federal mandate as part of an executive action by the governor, then promulgated it as a temporary rule by the Oregon Health Authority which later became a permanent rule. Washington had a similar state mandate that its governor ended last fall. On May 11, Oregon withdrew its vaccine mandate, but some states, such as New York, have kept theirs so far.

Even in the absence of a state or local mandate, "employers may want to evaluate whether it is prudent to implement or continue with an employer policy requiring COVID-19 vaccination going forward," Baumgart says.

On the other hand, you should review state and local ordinances on the subject thoroughly — some may be against mandates. "There are some states and municipalities that may bar vaccination requirements," Schmeltzer says, "so practices must keep that in mind before making the decision to continue with their employee vaccination policy."

You still may get sued

Experts agree that employees who have been let go for failing to vaccinate while the mandate has been in effect have little or no legal recourse unless their dismissal violated some other law or regulation. "A person's vaccination status is not a legally protected class" under federal discrimination laws, Schmeltzer says. "I am not concerned that disputes caused by the mandate will result in sanctions or damages against practices."

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:
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. *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: $699/year.

decisionhealth an hcpro brand

Even if some employees continue to protest their mandate-era dismissals, the end of the mandate shouldn't change their validity, Baumgart says. "The roll back of this mandate does not change the legal framework of pending COVID-related discrimination cases," she explains. "These cases will be evaluated based on the facts and circumstances that existed at the time any employment-related decision was made."

But when cases are filed post-mandate, they may be based on any of a variety of laws, such the Americans with Disabilities Act (ADA), "necessitating reasonable accommodations on the basis of religion and/or disability," Schaefer says. "We may see an uptick in claims and/or a dilution in defenses because the public health imperative is substantially different today than it had been."

Schmeltzer thinks some employees who lost their jobs for refusing to get vaccinated may sue. In New York, for example, a state supreme court judge has invalidated the state's mandate, though it remains in effect pending appeal, and this may provide an opening for ex-employees to sue under public health law that prohibits "mandatory immunization of adults or children." Schmeltzer is "skeptical" of their chances, but that doesn't negate the possibility that they'll try.

Facilities may decide, once the mandate lifts, to allow back employees they had dismissed. "For some, it will be important to defend their employment decisions at the time they were made, remembering the reality and health care imperative that existed at the time and that those decisions to suspend or terminate were not made lightly," Schaefer says. "Other organizations may feel less dug-in and more amenable to resolution through mediation or otherwise as time has passed."

Tell patients?

If you pull back on vaccination standards, should you tell patients? Experts agree this is a thorny question. On the one hand, "communication and transparency are critical, and even more so in the health care facility context," Schaefer says. "Patients will need and indeed will likely have a right to know about the practices at each facility so that they can make informed decisions about their own health and safety and personal comfort level."

On the other hand, there may be competing legal interests at play.

"In some practices, say oncology, where patients are often immunocompromised, the practice may want to consider notifying these patients that the practice no longer mandates COVID vaccination as a condition of employment," Schmeltzer says. "However, there are privacy concerns to consider. The U.S. Equal Employment Opportunity Commission [EEOC] has said that employee vaccination status is confidential medical information under the Americans with Disabilities Act. If a patient requests to be treated only by vaccinated employees, and the practice acquiesces, then the practice would be disclosing employee vaccination status to a third party."

Also, it may not make much sense to raise that flag now that health care facilities are cutting back on COVID precautions, DiVarco says. "Many hospitals have done away with mandatory masking throughout their health care facilities, [only requiring it] for certain patient care areas," she adds. "But no one is putting up signs, saying, 'guess what, we're not wearing masks anymore.'" — *Roy Edroso* (*redroso@decisionhealth.com*) ■

RESOURCE

- White House statement, "The Biden-Harris Administration Will End COVID-19 Vaccination Requirements for Federal Employees, Contractors, International Travelers, Head Start Educators, and CMS-Certified Facilities," May 1, 2023: www.whitehouse.gov/briefing-room/statements-releases/2023/05/01/the-biden-administration-will-end-covid-19-vaccination-requirements-for-federal-employees-contractors-international-travelers-head-start-educators-and-cms-certified-facilities/

Billing

How to capture the visit when key components drive split/shared billing

Medicare's rules for split/shared visits allow your care team to use the key components of a facility-based E/M visit to determine who performed the substantive portion of the encounter (*PBN 11/14/22*). But your physicians and qualified health care professionals (QHP) will need to carefully document each encounter, and your coders will need to review each chart with equal care.

Review the rules for each component

The provider who performs at least one key component of a visit — history, physical examination or medical decision-making (MDM) — will bill the visit with modifier **FS** (Split [or shared] evaluation and management visit).

When the substantive portion is based on the history or physical exam, "the billing practitioner must perform the [component] as described in the code descriptor," according to CMS 100-04, Change Request 13064. The descriptors for all level-based codes list a medically appropriate history and/or examination. Until CMS clarifies how it defines medically appropriate histories and physical exams, practices should check with their Medicare administrative contractor (MAC) for guidance.

When it comes to MDM, Medicare explicitly allows the providers to share the work. "If MDM is used as the substantive portion, each practitioner could perform certain aspects of MDM, but the billing practitioner must perform all portions or aspects of MDM that are required to select the visit level billed," CMS states in CR 13064.

The documentation will determine which provider's work supports MDM for the visit. **Example:** The practice bills a subsequent hospital visit with **99235**, which requires a moderate level of MDM. The QHP's documentation meets the requirements for 99235; the physician's documentation shows one ordered test and that the physician agreed with the QHP's findings. The QHP would bill the visit.

One provider must see the patient, both can contribute

Reassure staff that only one provider needs to see the patient when you bill a split/shared visit. In addition, "it does not necessarily have to be the physician, nor the practitioner who performs the substantive portion and bills for the visit. The substantive portion can be entirely with or without direct patient contact, and is determined by the proportion of total time, not whether the time involves patient contact," CMS states.

For example, the QHP could go to the facility and perform the history and physical exam. The physician could perform the MDM by reviewing test results, discussing the patient's care with providers from another group and deciding to perform surgery without leaving the office.

Make sure treating providers and coders understand that the documentation must support the performance of the substantive portion for each visit. Also, remember that agreeing with or signing off on another provider's work does not meet the requirements for the substantive portion. — *Julia Kyles, CPC* (*jkyles@decisionhealth.com*) ■

RESOURCE

- CMS 100-04, Change Request 13064: www.cms.gov/files/document/r11842cp.pdf

Practice management

Liability premiums up, again; wring value from carrier extras

Brace for some bad news: The AMA says a leading indicator of professional liability premium costs shows them going up. Consider shopping for better prices and avail carrier programs that can save you money.

Working with figures from the industry-standard Medical Liability Monitor (MLM) annual rate survey, the AMA finds that "2022 marks the fourth straight year in which the share of medical liability insurance premiums with a year-to-year increase was significantly higher than in the last two decades," according to its April 2023 Policy Research Perspectives report.

The numbers, distilled from manual premium prices for three specialties (OB/GYN, general surgery and internal medicine), show that 36.2% of liability insurance premiums increased from the previous year, and by an average of 8.1%.

The premium figures track with the AMA's finding last year that liability price volatility was reaching levels last seen in the early 2000s (*PBN 4/11/23*).

While "premiums had been increasingly stable through 2018, when 80.8% remained the same as in the previous year," report author José R. Guardado, Ph.D., writes, by 2022 "the proportion of premiums that remained the same fell to 56.1%." Also, 10.2% of premiums increased by 10% or more. The worst states for big jumps were Illinois, with 63.6% of premium increases being double-digit, New Mexico (33.3%) and Oregon (26.7%).

Beth Boone, a partner with Hall Booth Smith in Brunswick, Ga., says feedback from her clients tells her premiums are up "in a lot of sectors of the medical market — including medical malpractice, E&O and correctional health care."

Some of the change may be due to the COVID landscape, Boone says. "Folks weren't as busy during COVID and now their volume has increased, which could affect overall claims," she explains. At least part of it may just be inflation or changing business conditions.

(continued on p. 6)

Benchmark of the week

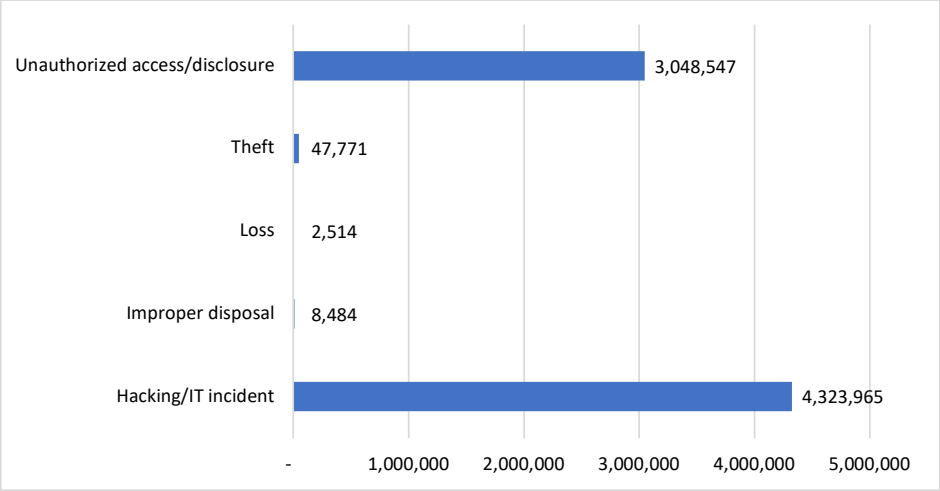
A year of HIPAA breach data highlights the current threats to PHI

Outside attempts to steal protected health information (PHI), such as ransomware attacks, dominate the headlines, but internal mistakes continue to trigger breaches involving at least 500 patients. Any provider who experiences a breach of that size must file a report with HHS that will be posted on the so-called HIPAA "wall of shame," notify the affected patients, make a public announcement, take steps to mitigate harm to the patients and, often, weather the bad press that follows.

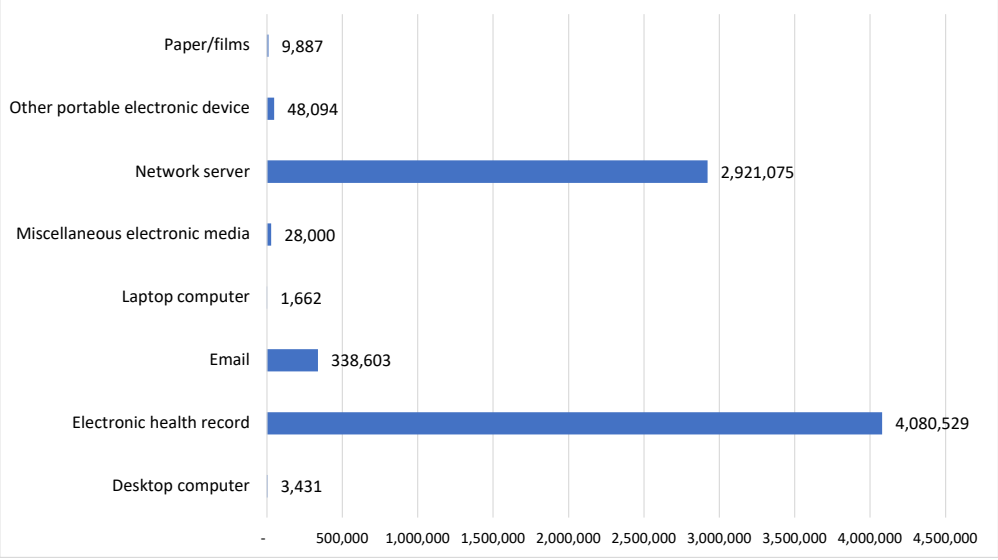
A review of the HHS Office for Civil Rights' (OCR) data for resolved breach reports filed from May 2022 to May 2023 shows that health care providers experienced hacking and other IT incidents that affected the PHI of more than 4.3 million individuals. Providers also reported unauthorized access and disclosure breaches that affected more than 3 million individuals. A single breach at a health system sent the PHI of 3 million patients to unauthorized individuals. However, medical and dental groups frequently reported lower-tech breaches that were caused by employees. Notes for the reports include breaches caused by employees who sent group emails to patients without using the blind carbon copy function, shared their passwords, or removed PHI from the practice for impermissible reasons.

The first chart shows the type of incident by total number of patients who were affected by the breach. The second chart shows the location of the PHI. Electronic health records (EHR) topped the list thanks to the health system breach, but network servers are a key point of vulnerability. – *Julia Kyles, CPC* (*jkyles@decisionhealth.com*)

Types of incident, May 2022-May 2023



Location of PHI, May 2022-May 2023



Source: HHS Office for Civil Rights breach portal: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

(continued from p. 4)

Check your benefits

If increases are getting too much for you, it may be time to shop for a new carrier or broker. Or you can take advantage of your current carrier's opportunities that you may have overlooked — for example, their risk management resources.

These include "very detailed and informative checklists and analysis of claims," Boone explains. "If your carrier's national, they'll have analyzed prior claims and lawsuits in your specialty, and they will have come up with ideas for their clients [in that specialty] on how to reduce risks. These could be based on trends in 'failure to diagnose' cases, for example, or 'failure to seek outside consult.'" Some carriers will send specialized risk management employees out to your practice to work on your case.

Also, Boone says, some carriers have discounts for providers who are a member of certain professional associations or entities, like the AMA. "They like clients to be active with these associations because it means they're attentive to standards of care," she says.

Changing carriers can be a difficult and frightening proposition, so see if you can't work these extras, and see what others your carrier can offer you, before making the leap. — *Roy Edroso* (*redroso@decisionhealth.com*) ■

RESOURCE

- AMA, "Policy Research Perspectives: Prevalence of Medical Liability Premium Increases Unseen Since 2000s Continues for Fourth Year in a Row": www.ama-assn.org/system/files/prp-mlm-premiums-2022.pdf

HIPAA

Implement 6 HIPAA security compliance tips for a strong 2023

HIPAA security remains a hot topic for medical groups, and federal agencies are warning of elevated threats to security. Pay attention to emerging practices that can help keep your data safe — and your money away from regulators.

Considering the spotlight that security of protected health information (PHI) has received in recent years, security expert Frank Ruelas, MBA, a compliance professional located in Casa Grande, Ariz., provides some compliance tips on the suggested areas of improvement. Implement the following six tips to stay protected.

- **Secure disposal**. More devices can contain ePHI compared to years past, Ruelas says.

In addition to the devices people often think about, such as thumb drives, smartphones or computers, there is also the entire class of objects that make up the internet of things (IoT).

"In my opinion, making sure that items are disposed of in a secure manner also means making sure that what needs to be disposed of is well identified and periodically inventoried," Ruelas says. "I don't necessarily see disposal as a challenge. Rather, I see the likelihood that things that need to be disposed of in a secure manner is getting greater, and the number and availability of these devices continues to grow."

Adopt the following tips:

  - Ensure secure disposal of electronic devices containing PHI.
  - HIPAA privacy officers should establish procedures to destroy PHI stored on electronic devices.
  - Remember that IoT devices can also contain PHI.
  - Regularly check for devices that need to be discarded.
- **Encryption**. Encryption is exceedingly significant, Ruelas says.

"However," he adds, "often these encryption functions need to be enabled by the user. It is interesting to me the reasons why I hear people do not make use of encryption. Often, the reason I hear is because using encryption adds extra steps or takes time. I like to remind people that the benefits of those few extra seconds or clicks on an encrypted device is a very good investment of time."

Encryption, combined with other security measures such as multifactor authentication, can significantly increase the protection of a device. Yet, those opposed to encryption will point out that it is not perfect, according to Ruelas.

"My response is that we aren't striving for perfection. Rather, we are striving to reach a level of reasonableness in protecting important information. To that end, I think encryption is something that must be used where and when it is possible to do so," Ruelas says.

Adopt the following tips:

- Encryption is a crucial tool in protecting PHI stored on electronic devices.
- Encryption functions are readily available but often need to be enabled by the user.
- Combining encryption with other security measures, such as multifactor authentication, increases its protection abilities.
- Despite its imperfections, encryption should be used whenever possible.

- **Employee training**. Training employees about HIPAA is helpful in several ways. First, it reminds everyone within the organization of the shared responsibility to keep patient information private and secure, according to Ruelas. This includes how to store, send and dispose of information in a manner that prevents breaches.

"Secondly, training contributes to the overall risk management process associated with complying with HIPAA," Ruelas adds. "Since we often hear that people are the weakest link in the chain of events or safeguards that protect the privacy and security of information, it stands to reason that effort must be taken to make this weakest link as strong as possible."

Adopt the following tips:

- It is vital to train employees on HIPAA regulations and privacy practices.
- Regular training for all employees ensures everyone is on the same page about keeping patient information private and secure.
- Training is part of the overall risk management process associated with HIPAA.

- **Regular risk assessments**. HIPAA privacy officers should conduct regular risk assessments to identify potential vulnerabilities in their organization's privacy and security practices, according to Ruelas. Regular risk assessments help pinpoint areas for improvement and can prevent HIPAA violations.

"One result that comes from a well-done risk assessment is the identification of gaps that may represent possible vulnerabilities to an organization's information system," Ruelas says. "There may be many reasons contributing to a gap, which I describe as the difference between the current state and the desired state."

Regular risk assessments are crucial to verify whether new applications and programs remain in accordance with the facility's security safeguards, Ruelas adds.

"It is not uncommon to hear that a breach or other issue occurred in connection with a computer application or program that was never reviewed by those that oversee the security program within an organization," Ruelas says. "Conducting risk assessments, and just as importantly, reviewing them regularly to make sure they are accurate and thorough, are critical in identifying areas for improvement."

Adopt the following tips:

- HIPAA privacy officers should conduct risk assessments regularly to identify potential vulnerabilities and areas for improvement.
- Regular review of assessments ensures accuracy and thoroughness.
- Risk assessments help identify gaps in security safeguards and possible vulnerabilities.

- **Incident response plan**. "In my opinion, the effectiveness and efficiency of dealing with violations is a function of the process pathway that these violations are discovered and reviewed, and then whatever resulting actions are identified and completed," Ruelas says.

"Without a plan or a road map to complete these steps, I think at best an incident response plan is destined to be a hit-or-miss proposition. Sometimes things may go well, and sometimes they may not. I don't believe many compliance professionals would have much confidence in a less than well-defined process to handle incidents," he adds.

Adopt the following tips:

- Developing a comprehensive incident response plan is crucial to handle potential HIPAA violations effectively and efficiently.
- An incident response plan should be a road map with defined steps and processes.

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.

- **Breach notification**. HIPAA regulations require organizations to notify individuals when a breach affects their PHI. HIPAA privacy officers should ensure that their organization has a process for quickly and effectively providing breach notification to affected individuals.

"The best time to rehearse for a 'what if' scenario regarding the need to notify individuals whose information is involved in a breach is before that 'what if' happens, in my opinion," Ruelas says. "For the most part, I would [divide] the plan into two categories. One is for breaches of less than 500 affected individuals, and the other plan for 500 or more affected individuals."

The plan for 500 or more includes breaches that could involve hundreds or thousands of affected individuals, but responses to such major breaches can be developed as needed after identifying the type of notification each of the two plans would require.

"By rehearsing these plans," Ruelas adds, "those involved in managing the process are practicing without the pressure of actual deadlines, which could cause anxiety and confusion easily resulting in errors."

Adopt the following tips:

- HIPAA regulations require organizations to notify individuals in case of a breach.
- HIPAA privacy officers should have a predetermined plan to provide breach notifications to affected individuals.
- The plan should include a scenario for breaches involving fewer than 500 and more than 500 affected individuals. — *Dom Nicastro* (*pbnfeedback@decisionhealth.com*) ■

RESOURCES

- OCR, Improving Cybersecurity Posture in Healthcare for 2022: www.hhs.gov/blog/2022/02/28/improving-cybersecurity-posture-healthcare-2022.html
- HHS Security Risk Assessment Tool: www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool
- OCR, request for information: www.hhs.gov/hipaa/for-professionals/regulatory-initiatives/hitech-rfi/index.html

Ask Part B News

Report the right E/M level for ED patient with exacerbated chronic illness

Question: *A 19-year-old male with asthma who experienced wheezing and shortness of breath for the past two weeks presented to the emergency department (ED). Inhaler use 10-14 times daily offered temporary relief. Physical exams were normal except for tachycardia, scattered wheezing breath sounds, and elevated respiration. The physician completed three tests (complete blood count; complete metabolic panel; influenza A/B, respiratory syncytial virus, and COVID-19 polymerase chain reaction panel), gave the patient a nebulizer treatment and steroids, released him with MDI and steroid burst, and referred him for a follow-up visit with his doctor of primary medicine. Which CPT code would be reported for this visit?*

Answer: This scenario fits quite neatly into the requirements for CPT code **99284** (ED visit for the E/M of a patient, which requires a medically appropriate history and/or examination and moderate level of medical decision-making [MDM]), according to the American Medical Association's ED MDM grid.

The patient has a chronic illness with exacerbation, which is a moderately complex problem. The physician ordered three tests and reviewed those results, which supports a moderate level of MDM. Then the physician gave the patient a prescription drug, which also supports a moderate level of MDM.

This encounter, therefore, would be reported using CPT code 99284 for an ED visit. When coding ED visits, if the provider sees a patient with an exacerbation for a chronic illness, coders should make sure that he or she documents whether the exacerbation is severe. That documentation is going to be the differentiation between moderate and high complexity for the problems addressed. — *Savannah Schmidt* (*pbnfeedback@decisionhealth.com*) ■

Editor's note: *Shannon E. McCall, RHIA, CCS, CCS-P, CPC, CPC-I, CEMC, CRC, CCDS, CCDS-O, director of HIM and coding for HCPro in Middleton, Massachusetts, answered this question during the HCPro webinar "2023 E/M Update: Guideline and Reporting Changes Come to Observation and ED Services." Learn more: https://codingbooks.com/yhha010523.*