



# Home Health Line

Regulatory news, benchmarks and best practices



## In this Issue

- 1 **Compliance**  
OIG announces plans to look at how agencies are using telehealth services
- 3 **Infection control**  
Double up on COVID-19 education to comply with new OSHA rules
- 4 **COVID-19: Coding**  
Understand & assign the new codes to capture COVID-19 conditions
- 6 **Safety compliance**  
Expert answers question about logging COVID-19 exposure
- 7 **HIPAA compliance**  
Protect your agency against an increase in HIPAA and security threats
- 8 **Benchmark of the week**  
Data show use of new COVID-19 codes

### Compliance

## OIG announces plans to look at how agencies are using telehealth services

Home health services conducted via telehealth during the COVID-19 pandemic will be audited by the Office of the Inspector General (OIG) according to a recent announcement that has left home health agencies, and consultants that work with them, wondering why the government would audit services that are not reimbursable by CMS.

“I’m not sure what the purpose of the audits would be,” says Laura Page-Greifinger, a consultant with McBee Associates in Floral Park, N.Y. Maybe it’s to check the number of virtual visits versus face-to-face ones and to make sure agencies are following the plan of care, she says.

Arlene Maxim, CEO of A.D. Maxim Enterprise in Fort Lauderdale, Fla., agrees that the OIG is likely looking to see if the telehealth services are included in the plan of care. Also, she ventures that the audit likely aims to determine if agencies are billing for virtual visits, even if accidentally.

The OIG doesn’t comment on reports before they are written, says Donald White, an OIG spokesman. But White did caution not to make any assumptions about what the announcement means, noting that the report won’t come out until 2022. White also pointed out that the audit is of home health services not home health agencies.

The announcement highlights a topic that is a sore spot in the industry, as experts agree the time has come for CMS to recognize and appreciate the value of these virtual visits. Among the advantages of telehealth, experts say, are lower overall cost of care, less money and time spent on transportation and reduced re-hospitalizations.

## Navigate the new norms of a home health administrator

Join us August 16-18, 2021, at the **Home Health Administrator’s Summit** in Las Vegas as the nation’s thought leaders and agency heads come together to reflect on a challenging year and identify the steps necessary to leverage the new-found importance of home health in the post-pandemic world. For more details and to register, visit <https://store.decisionhealth.com/conferences/>.



Outcomes for services that use telehealth are much more favorable than those that don't use telehealth, Maxim says. She notes that her company, with more than 100 provider clients across the nation, encourages the use of this technology.

"Telehealth has struggled to get off the ground in our industry, because it's not reimbursable," says Sharon Litwin, senior manager, coding and clinical consulting, for Nashville-based Healthcare Provider Solutions Inc. "It should have been allowed years ago."

With the pandemic opening up telehealth options among medical professionals, industry experts see now as a crucial time for home health to plead their case. The National Association for Home Care is pushing hard on this topic and trying at the very least to have telehealth visits count towards Low Utilization Payment Adjustment (LUPA), Litwin says.

"The pandemic has changed doctors' reticence to use telehealth," Page-Greifinger says. "Smart agencies use telehealth. It offers less visits with better outcomes and you're not spending so much. It's a win-win. Patients love it. Staff are happy. I do see great things coming out of telehealth. I think CMS is seeing the benefits, and we will be reimbursed for it down the road."

## Telehealth improves outcomes

Concierge Home Care in Jacksonville, Fla., has been using telehealth since 2017, says Linda Murphy, co-founder and chief operating officer for the agency that has 13 offices throughout Florida with six more opening in the next few months.

The agency absorbs the cost (\$80 to \$120) of supplying electronic devices to clients that need it. That includes the cost of blood pressure cuffs, pulse oximeters, peak flow meters or blood glucose monitors, she says. But the benefits are that "we are moving the needle in reducing rehospitalizations," she adds.

Using a communication application platform from Synzi, St. Petersburg, Fla., telehealth visits help Concierge Home Care do assessments and reinforce education.

This technology helps the agency ensure that face-to-face visits, text messaging and emailing are all HIPAA compliant, Murphy says. "We are trying to use technology to its fullest."

With patients concerned about letting people into their homes and doctors now using telehealth medicine themselves, the onset of the COVID-19 pandemic has actually aided Murphy's efforts.

"COVID helped us expand our program to another level," she says. "We've made our virtual visits more meaningful with separate nursing notes and therapy notes. Significant time is spent on each virtual visit, and we are hopeful CMS will see the value in these virtual visits in preventing rehospitalization."

decisionhealth  
an hcpro brand

## SUBSCRIBER INFORMATION

Have questions on a story? Call or e-mail us.

### EDITORIAL

Have questions on a story? Call toll-free: 1-855-CALL-DH1

### HOME HEALTH LINE TEAM

**Maria Tsigas, x6023**  
Product Director  
[mtsigas@decisionhealth.com](mailto:mtsigas@decisionhealth.com)

**Marci Geipe, x6022**  
Senior Manager, Product and Content  
[mgeipe@decisionhealth.com](mailto:mgeipe@decisionhealth.com)

**Greg Hambrick X6024**  
Associate Content Manager  
[ghambrick@decisionhealth.com](mailto:ghambrick@decisionhealth.com)

**Megan Herr, x4062**  
Content Specialist  
[mherr@decisionhealth.com](mailto:mherr@decisionhealth.com)

Join our DecisionHealth — Home Care Matters community!

[www.facebook.com/DecisionHealthPAC](https://www.facebook.com/DecisionHealthPAC)

[www.twitter.com/DH\\_HomeCare](https://www.twitter.com/DH_HomeCare)

[www.linkedin.com/groups/12003710](https://www.linkedin.com/groups/12003710)

### PLEDGE OF INDEPENDENCE

At DecisionHealth, the only person we work for is you, the provider. Home Health Line is not affiliated with any special interest groups, nor owned by any entity with a conflicting stake in the healthcare industry. For nearly three decades, we've been independently watching out for the financial health of healthcare providers, and we'll be there for you and your peers for decades to come.

### WEBSITE

[www.homehealthline.com](http://www.homehealthline.com)

### SUBSCRIPTIONS

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

### ADVERTISING

To inquire about advertising in HHL, call Amy Roadman, 1-855-CALL-DH1 x8119.

### COPYRIGHT WARNING

Copyright violations will be prosecuted. Home Health Line 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 our copyright attorney Brad Forrister at 1-800-727-5257 x8041 or email [bforrister@blr.com](mailto:bforrister@blr.com).

### REPRINTS

To request permission to make photocopy reprints of Home Health Line articles, call 1-855-CALL-DH1 or email customer service at [customer@decisionhealth.com](mailto:customer@decisionhealth.com). Also ask about our copyright waiver, multiple copy and site license programs by calling the same number.

Home Health Line is a registered trademark of DecisionHealth. Home Health Line is published 48 times/year by DecisionHealth, 100 Winners Circle, Suite 300, Brentwood, TN 37027. ISSN 0893-8121. Price: \$627/year. © 2021 DecisionHealth

decisionhealth  
an hcpro brand

## Tips for compliant telehealth use

Some practical ways agencies can ensure compliant telehealth use and improve documentation:

- **Hire a project manager.** “Implementing a new process is a lot bigger undertaking than you think,” Murphy says. “It’s a culture shift for staff. You should have a separate virtual health team and field staff.”
- **Assign remote care coordinators.** These employees would be responsible for gathering data such as blood pressure monitoring and weight, not interacting with patients, making it easier for those actually conducting the virtual visits, Maxim says.
- **Create virtual visit notes.** Contact your Electronic Medical Record (EMR) company and have them design a telehealth specific record. There should be templates for telehealth visits, Murphy says. Not only will this ensure there is no confusion between virtual and hands-on visits, it will help drive the value of virtual visits in the overall plan of care, experts say.
- **Produce clear guidelines and protocols.** Telehealth visits are more than just check-in visits, Murphy says. “You are accomplishing a set of goals on the care plan for each visit.”

Page-Greifinger says it’s important that the plan of care tells the story of the patient and that each visit, whether in-person or virtual, should add to that story. Additionally, teaching tools are embedded in telehealth for patients who need education to take control of their own health.

- **Research Health Insurance Portability Accountability Act (HIPAA)-compliant telehealth technology now.** “Right now we can use non-HIPAA compliant resources like Skype and FaceTime for our virtual visits,” Maxim says. “Once the pandemic is over, we lose that option and the technology has to be HIPAA-compliant. Research that now while you have the time.”

A few of the leading HIPAA-compliant telehealth vendors in home health care are Connected Home Living, which offers remote care monitoring with 24-hour live virtual assistance; Vivify, which has remote care monitoring data only; Synzi, which offers virtual care data only; and Health Recovery Solutions. — *Annmarie Sarsfield Edwards* ■

## Infection control

### Double up on COVID-19 education to comply with new OSHA rules

New workplace guidance on COVID-19 from the Occupational Safety and Health Administration (OSHA) offers an important reminder that employee education on PPE and pandemic protocols is critical. That is particularly true in an industry with so many staff members working remotely, according to experts on infection control and compliance.

The new OSHA guidance, released January 29, notes an effective COVID-19 prevention program includes 16 elements focused on identifying and addressing potential risks of exposure while protecting employees and incorporating their input. This guidance may be in advance of mandatory OSHA policies in the next few months ([HHL 2/15/21](#)).

#### Find your staff’s COVID-19 leader

The first item OSHA notes in its guidance for a prevention program is an effective leader. Employers should assign a “workplace coordinator” who will be responsible for COVID-19 issues on the employer’s behalf.

Considering rules already in place for emergency preparedness and infection control, most agencies already have the right person on staff, notes Diane Link, owner of Link Healthcare Advantage of Littlestown, Pa.

The COVID-19 coordinator could be the same person who oversees the infection control program, she says. Usually, that’s the Quality Assurance & Performance Improvement (QAPI) manager or clinical manager.

Their responsibilities may be similar to what they already do, including gathering data for all COVID-19 patients and staff, educating on infection control and verifying that staff are documenting screenings and educating patients, Link says. “The only other thing added would be monitoring PPE on hand.”

#### 4 tips for safe respirator use

Another important part of the OSHA guidance focuses on employee education.

Employers should be training workers on COVID-19 policies and procedures “in plain language that workers understand,” OSHA notes, while stressing employers should use multiple methods to educate staff.

When working with client home health agencies, their staff often are unable to answer key questions, says infection control expert Mary McGoldrick, a home care and hospice consultant based in Naples, Fla, and the author of the *Home Care Infection Prevention and Control Program* manual.

McGoldrick tells *HHL* that employers should make sure they’re educating staff on these key protocols:

- **Limit the number of times you can don a respirator.** This is going to depend on the manufacturer guidance, according to the Centers for Disease Control and Prevention (CDC). However, the general guideline is to avoid reusing more than five times.
- **Track respirator use.** A paper bag can serve as an easy container to store your respirator. But it also can serve as a place to log uses, McGoldrick notes. Employees also should make sure the container is disposed of or cleaned regularly, she says.
- **Perform a user seal check each time after donning the respirator.** A user seal check involves blocking the air paths while inhaling or exhaling. McGoldrick says she has seen staff put on the mask and pinch the nose, but then forget the seal check.
- **Know when to dispose of the respirator.** Regardless of the maximum number of allowed uses, there are times when a respirator should be disposed of. They include aerosol generating procedures, when the respirator has been soiled or damaged or when contaminated with blood, or other bodily fluids from the patient, according to the CDC.

### Watch staff demonstrate PPE use

During a recent webinar for the National Association for Home Care and Hospice (NAHC), McGoldrick also noted employers need to test staff competency on PPE protocols.

She said staff have told her that they have had their competency “checked,” but that no one watched them put on and take of the PPE.

Keep these other issues in mind:

- **Respirator introduction.** Staff members need to have the full training required by OSHA on respirator use, and they need to be fit-tested for the make, model and style of the respirator that they are going to wear in the home during visits, McGoldrick says.
- **Appropriate face masks.** In situations where face masks are an acceptable alternative to N95s, make sure that the masks provided to staff are of a quality that will keep them safe. Not every “blue” mask is equal. The box should have an ASTM label of “Level 3,” indicating it’s a surgical mask that is approved by the Food and Drug Administration, McGoldrick says.
- **Face shield positioning.** “When I’m out with staff, a common issue I see is that they wear their face shield like a baseball cap,” McGoldrick says. You should wear the mask around your head, just above the eyebrows. It should come down below your chin and curve around your ears. When removing, don’t touch the front of the shield. Clean from the inside out.
- **Handling tablets, cell phones and laptops.** Whatever clinicians are having the patient sign for the electronic visit verification needs to be cleaned or disinfected prior to handing to the patient or they need to provide hand sanitizer to the patient for them to immediately sanitize their hands after handling a tablet. — Greg Hambrick ([ghambrick@decisionhealth.com](mailto:ghambrick@decisionhealth.com)) ■

**Related links:** For more on CDC respirator recommendations, visit <https://bit.ly/2Nm1IU1>.

### COVID-19: Coding

## Understand & assign the new codes to capture COVID-19 conditions

By Sharon Litwin

Implementing a new code to capture COVID-19 in April 2020 was, of course, necessary. However, the changing guidelines and lack of clarification made it challenging for coders to assign all of the correct diagnosis codes.

Failure to correctly code the virus and related conditions could have a negative effect on your clinical and financial outcomes.

Under PDGM, the code for COVID-19 remains U07.1 (COVID-19). The Clinical Group it is assigned to is MMTA — Medication Management, Teaching & Assessment

— Respiratory, and it falls into the Respiratory 10 comorbidity group.

The Centers for Disease and Infection Control and Prevention (CDC) also created codes for both active COVID-19 and post-COVID-19-related conditions — as many of the long-term effects of the novel Coronavirus became known. They took effect Jan. 1.

The new 2021 COVID-19 ICD-10 codes are:

- **J12.82** (Pneumonia due to coronavirus disease 2019)
- **M35.81** (Multisystem inflammatory syndrome (MIS))
- **M35.89** (Other specified systemic involvement of connective tissue)
- **Z11.52** (Encounter for screening for COVID-19)
- **Z20.811** (Contact with and (suspected) exposure to COVID-19)
- **Z86.16** (Personal history of COVID-19)

*Note: For a benchmark showing how often these codes appeared on claims in January, see p. 8.*

## Pneumonia due to COVID-19

The new code to capture pneumonia due to COVID-19 is J12.82 (Pneumonia due to coronavirus disease 2019).

This respiratory diagnosis code is assigned secondary following U07.1 as coding guidelines state to code COVID-19 first.

J12.82 cannot be a primary diagnosis as it states it is “due to” coronavirus.

Prior to Jan. 1, without this more specific code, J12.89 (Other viral pneumonia due to COVID-19) was assigned. But coders should not use J12.89 to code pneumonia due to COVID-19 on any claims with a “from date” beginning January 1, 2021.

## 2 new musculoskeletal codes

Two new musculoskeletal codes were also added as part of this update. They are:

### 1. **M35.81 (Multisystem inflammatory syndrome)**

Other terms are Multisystem inflammatory syndrome in adults (MIS-A), Multisystem inflammatory syndrome in children (MIS-C) and Pediatric inflammatory multisystem syndrome (PIMS).

Coding guidelines for M35.81 state to code first, if applicable, COVID-19 (U07.1) and also code for any associated complications such as:

- K72.0- (Acute hepatic failure)
- N17.- (Acute kidney failure)
- I40.- (Acute myocarditis)
- J80 (Acute respiratory distress syndrome)
- I47-I49.- (Cardiac arrhythmia)

*Note:* If COVID-19 is not coded as the primary diagnosis, then the applicable codes of exposure to COVID-19 would be coded. That includes Z20.822 (SARS-CoV-2 infection), Z86.16 (Personal history of COVID-19 (Z86.16) or B94.8 (Sequelae of COVID-19).

### 2. **M35.89 (Other specified systemic involvement of connective tissue)**

Currently, there are no specific guidelines for this diagnosis code. Therefore, physician documentation will state M35.89 as the diagnosis and any additional codes will follow the coding guidelines.

## 3 new Z codes

### 1. **Z11.52 (Encounter for screening for COVID-19)**

This code has a note in the coding guidelines which states, “During the COVID-19 pandemic, a screening code is generally not appropriate. Do not assign code Z11.52 (Encounter for screening for COVID-19). For encounters for COVID-19 testing, including preoperative testing, code as exposure to COVID-19.”

*Note:* Keep in mind that while this code does fall into a clinical group (MMTA- Other), it is not appropriate for assignment based upon the above guideline. If a home health agency is performing COVID-19 testing, then code Z20.811(Contact with and (suspected) exposure to COVID-19) until further updates to the guidelines occur.

### 2. **Z20.822 (Contact with and (suspected) exposure to COVID-19 (SARS-CoV-2))**

Coding guidelines state that three categories would be coded to Z20.822:

- Asymptomatic individuals with actual or suspected exposure to COVID-19
- Symptomatic individuals where the infection has been ruled out

- Patients whose test results are inconclusive or unknown

If an individual with a known or suspected exposure to COVID-19, without current COVID-19 infection or history of COVID-19, develops MIS, assign codes M35.81 (Multisystem inflammatory syndrome) and Z20.822 (Contact with and (suspected) exposure to COVID-19).

### 3. Z86.16 (Personal history of COVID-19)

There is an excludes 1 note that includes sequelae of infectious and parasitic diseases (B90-B94). Therefore, when there is sequelae of COVID-19, the personal history code would not be coded.

**Note:** There are no timeframes stated in the coding guidelines for when to assign Z86.16 rather than active COVID-19. In addition, there is no timeframe for when to code sequelae rather than active COVID-19. Therefore, it is critical to follow the physician's documentation and to query the physician if there is no documentation stating this information.

### 3 codes that can be primary

Three of the new codes can be assigned as a primary diagnosis in home health. They are:

1. **M35.81 (Multisystem inflammatory syndrome)**, which falls into the musculoskeletal rehabilitation clinical group
2. **M35.89 (Other specified systemic involvement of connective tissue)**, which falls into the musculoskeletal rehabilitation clinical group
3. **Z20.822 (Contact with and (suspected) exposure to COVID-19)**, which falls into the MMTA — Infectious disease, neoplasms and blood-forming diseases clinical group

**Reminder:** While Z11.52 (Encounter for screening for COVID-19) does fall under the MMTA — Other clinical group, it is not appropriate for primary assignment based upon coding guidelines.

Two of the new codes were not assigned to a clinical group, so they cannot be assigned as a primary diagnosis. They are:

- **J12.82** (Pneumonia due to coronavirus disease 2019)
- **Z86.16** (Personal history of COVID-19)

J12.82 (Pneumonia due to coronavirus disease 2019) is the only new diagnosis that was assigned to a comorbidity group — Respiratory 2. ■

**About the author:** Sharon Litwin, RN, HCS-D, is senior manager of coding and clinical consulting with Healthcare Provider Solutions in Nashville, Tenn.

### Safety compliance

## Expert answers question about logging COVID-19 exposure

By Kelsey Heino, Goosmann Law Firm

**Q: One of our nursing home employees who was exposed to a COVID-19-positive resident just returned to work from a 14-day quarantine after testing negative. Do we have to record it in the Occupational Safety and Health Act (OSH Act) logs?**

**A:** Under current Occupational Safety and Health Administration (OSHA) guidance, employers are only responsible for recording cases of COVID-19 if all of the following are true:

- It is a confirmed case of COVID-19;
- It is work-related; *and*
- It involves one or more of the general recording criteria set forth in the regulations (e.g., medical treatment beyond first aid, days away from work).

Based on the scenario presented in your question, you wouldn't need to record the exposure on your OSH Act log, because the employee didn't contract COVID-19 despite having been exposed in the course and scope of employment.

Conversely, you would need to report the incident on your OSH Act log if the employee was diagnosed with COVID-19 and met any of the following recording criteria:

- Days away from work;
- Restricted work or transfer to another job;
- Medical treatment beyond first aid;
- Loss of consciousness; or
- A significant injury or illness diagnosed by a physician or other licensed healthcare professional, even if it doesn't result in death, days away from work, restricted work or job transfer, medical treatment beyond first aid, or loss of consciousness.

It's prudent for employers to keep a log of all COVID exposures even if, as in this instance, an exposed employee is asymptomatic and/or receives a negative test result. Keeping a log of exposures can be eminently useful in case it's later determined the employee was an asymptomatic carrier who received a false negative (or simply took the test too soon or late to receive a positive result) and exposed other colleagues. ■

*About the author:* Kelsey Heino is an employment attorney with the Goosmann Law Firm in Sioux Falls, S.D. You can reach her at 402-315-1241 or [heinok@goosmannlaw.com](mailto:heinok@goosmannlaw.com).

## HIPAA Compliance

# Protect your agency against an increase in HIPAA and security threats

Now more than ever, the severity of cyberthreats, and the frequency with which they are attacking health care organizations, has continued to increase at an alarming rate.

Here are a few questions about HIPAA trends answered by some of the leading experts on this topic.

### **Q: What are the greatest challenges that lie ahead for the privacy and security of health information?**

**A:** The greatest challenge facing health care is the invisible villain's intent on disrupting operations for ransom, says Michael Caplenor, director of client security assurance at CereCore in Nashville, Tenn.

"We have many controls available to limit the impact and access of these threats into our networks, but we are still vulnerable to user error and malicious insiders," he says.

Without question, the frequency of cyberattack attempts will continue to rise. It's imperative that providers stay on top of the updates and the types of attacks that are occurring, says Angela Rose, MHA, RHIA, CHPS, vice president of implementation services for MRO Corp. in Norristown, Pa. This means taking publicly available information — such as the recent HHS, FBI and CISA joint advisory — and using it to update policies, tools and response plans.

This year, agencies are faced with tackling these threats while dealing with a lack of resources.

"The pandemic has only served to exacerbate the limitations in need of resources," Blass says. "The solution is not easy when there are such limitations and constraints; however, periodic security risk assessments (SRAs) can help health care organizations to prioritize their resource needs on areas that represent their biggest risks. The good news is that we have observed improvements with this kind of ongoing strategy, which should result in the implementation of better and more privacy and security controls over time, especially for smaller healthcare organizations."

**Q: Cybercrime perpetrated against health care organizations seems to be rising — and rapidly. Check Point Research discovered a 50% increase in the daily average of ransomware attacks during Q3 of 2020. With employees working remotely, health care organizations are at an even greater risk. Going forward, what are the industry's greatest vulnerabilities when it comes to cyberattacks? What immediate and long-term steps should organizations take to mitigate risk and fill in the gaps for some of these vulnerabilities?**

**A:** "Humans will always be an organization's greatest vulnerability," says Kate Borten, CISSP, CISM, HCISPP, founder of The Marblehead Group in Marblehead, Mass. "We can teach our workforce about phishing and test their response through simulated attacks, and most people will eventually get it. But there will continue to be both sophisticated attacks and people who miss the clues because they are rushed or distracted or simply fooled."

Angela Rose, MHA, RHIA, CHPS, vice president of implementation services for MRO Corp. in Norristown, Pa., notes three vulnerabilities including human error and judgment, staying current both within your network infrastructure and with what's happening in the environment and lack of education and training.

In terms of staying current, Rose recommends changing passwords more frequently and auditing user activity more often than before. Key education and training strategies include sending phony phishing emails to the workforce and using this to identify gaps and provide further training as needed, Rose says.

According to Kevin Beaver, CISSP, independent security consultant at Principle Logic LLC in Atlanta, proper patching of networks remains a key issue in many health care organizations.

“Some say that certain systems cannot be touched and are therefore out of scope for system maintenance,” Beaver says. “This is the heart of the problem, especially in hospitals in larger clinics. I guess it ultimately boils down to priorities. You work together to find a solution on patching antiquated systems or otherwise keeping them protected, or you move on as before. To me, the consequences of ignoring this issue are much greater than the risks associated with taking the systems offline periodically to do proper maintenance.”

Michael Caplenor, director of client security assurance at CereCore in Nashville, Tenn., discussed a layered security approach that includes the following steps:

- **Limit entry.** This begins with messaging and email solutions that identify and filter messages for junk and security threats. Such solutions will commonly block and strip malicious links, attachments or defined “hostile” domains, flag any messages from outside email domains as #EXTERNAL#, and insert a header on your email messages that warns the message is not from inside the company. Implementing multifactor authentication is also critical.
- **Educate.** Educate users continuously on new and emerging threats, train them on spotting the signs and characteristics of a phishing attack, use a

mechanism to test their phishing awareness through focused and contemporary attacks that mimic real-world attacks, and provide a mechanism for staff to report phishing emails that get through your messaging entry layers.

- **Limit spread.** Stay current on patches for systems to limit common vulnerabilities that allow entry and escalation of privileges, maintain current operating systems and implement a privileged access management (PAM) strategy that randomizes usernames and passwords of all workstation and server local admin accounts and controls or “locks” admin group access so that if one asset is compromised, that compromise does not include all other networked assets.
- **Recover.** Viruses can spread to and corrupt backups, so organizations should maintain off-site backup copies, air-gapped backups and immutable storage to ensure their backups are not corrupted by a virus or ransomware, says Caplenor. Increasing the frequency of backups and recovery points will reduce recovery “loss.” — *Kevin Duffy* ([kduffy@hcpro.com](mailto:kduffy@hcpro.com)) ■



## Benchmark of the Week

### Data show use of new COVID-19 codes

About 10% of a total 523,986 primary codes were COVID-19 related in January 2021, the first month they took effect. J12.82 (Pneumonia due to coronavirus disease 2019) was the most commonly used of these codes, used 69 times as primary and 27,011 times as secondary. The data reflect starts of care and resumptions of care from Strategic Healthcare Programs (SHP) National Client Database.

While the code Z11.52 did appear a total of 107 times, it should be noted that current ICD-10-CM coding guidelines state that because the pandemic is ongoing, “a screening code is generally not appropriate. Do not assign code Z11.52 (Encounter for screening for COVID-19). For encounters for COVID-19 testing, including preoperative testing, code as exposure to COVID-19.” Exposure to COVID-19 is coded by assignment of Z20.822. (See *story, p. 4, for how to code COVID-19.*)

ICD-10 code	Code description	Primary	Secondary	Total
U07.1	COVID-19	51,718	11,818	63,536
J12.82	Pneumonia due to coronavirus disease 2019	69	27,011	27,080
M35.81	Multisystem inflammatory syndrome (MIS)	9	29	38
M35.89	Other specified systemic involvement of connective tissue	6	10	16
Z11.52	Encounter for screening for COVID-19	9	98	107
Z20.822	Contact with and (suspected) exposure to COVID-19	54	312	366
Z86.16	Personal history of COVID-19	34	1,863	1,897

**Source:** Strategic Healthcare Programs (SHP) National Database