December 2020 | Volume 31, Issue 12

Medical Practice Compliance Alert

News, tools and best practices to assess risk and protect physicians

In this issue

DecisionHealth
a Simplify Compliance brand

New regulations

Stark, anti-kickback rules reduce compliance load, but read the fine print

By Julia Kyles, CPC

Here's some good news to end the year: The new rules that update the Stark physician self-referral law and the Anti-Kickback Statute should make it easier for practices to stay in compliance with the expansive anti-fraud laws.

The Medicare Program; Modernizing and Clarifying the Physician Self-Referral Regulations rule "opens additional avenues for physicians and other healthcare providers to coordinate the care of the patients they serve — allowing providers across different healthcare settings to work together to ensure patients receive the highest quality of care," CMS announced in a fact sheet released Nov. 20, the same day the rule was released.

"The regulatory changes are aimed at reducing barriers to care coordination and value-based arrangements in order to help accelerate the transformation of the nation's health care system to one that incentivizes providers to focus on improved quality, better health outcomes and increased efficiency in health care delivery," says Laura Morgan, attorney, Dorsey & Whitney, Minneapolis.

Health care stakeholders — including medical practices — were reluctant to enter care coordination arrangements that didn't fit an existing exception under Stark or a safe harbor under the Anti-Kickback Statute. The rules are designed to ease those concerns and reduce the regulatory burden of compliance, Morgan says.

For example, "under Stark's new sections on value-based activities physicians and other providers can align with a health system and exchange remuneration (money or services) as long as they fit the exception. Right now under Stark you would have to try to protect arrangements under the personal services exception," but that has limited applicability because it would have to cover so many members, says Nicole Aiken-Shaban, counsel, Reed Smith, Philadelphia.

Another example: "If a hospital revised its care protocol for screening for a certain type of cancer based on guidelines from a nationally recognized organization, the hospital could enter into contracts with physicians to compensate the physicians $10

for each instance that they order testing in accordance with the new screening protocol over a two-year period. While this would not meet any existing Stark exceptions, this could be structured to meet the new Stark exception for value-based arrangements," says Alissa Smith, partner, Dorsey & Whitney, Des Moines, Iowa.

The HHS Office of inspector General (OIG) made a similar statement about its Revisions to the Safe Harbors Under the Anti-Kickback Statute and Civil Monetary Penalty Rules Regarding Beneficiary Inducements rule, which was also released Nov. 20.

"This Final Rule is part of HHS's Regulatory Sprint to Coordinated Care (Regulatory Sprint), which aims to reduce regulatory barriers to care coordination and accelerate the transformation of the health care system into one that better pays for value and promotes care coordination," the OIG said in a fact sheet issued on the same day.

Both rules go into effect Jan. 19, 2021, with one exception: The revision to Stark's exception for productivity bonuses and how they are distributed in group practices (§411.352[i]) will go into effect Jan. 1, 2022, says Aiken-Shaban.

Upgrades go beyond value-based programs

CMS and the OIG emphasized that the revisions align the rules with the shift to value-based payment models, such as accountable care organizations (ACO). But health care attorneys note that there's much more to the new rules.

"While a huge portion of these rules are related to the safe harbors and exceptions, there are many other changes that have been implemented as a result of these final rules," says attorney Karen Lovitch, chair of health law practice for Mintz, Washington, D.C. "Generally speaking, there are many changes that are intended to offer flexibilities … and to provide more certainty especially in relation to Stark," Lovitch says.

"With respect to Stark there were also a number of revisions that relate to modernizing and clarifying existing definitions in the Stark law," Aiken-Shaban says.

The updates to Stark include "critically necessary guidance related to fundamental concepts under the Stark Law — specifically, fair market value, commercial reasonableness, and compensation not being determined in a manner that takes into account the volume or value of referrals," Morgan says.

"I think it is bit misleading — the top-of-the-fold headlines that say this is all about value based enterprises," says Clinton Mikel, partner, Health Law Partners, Farmington Hills, Mich."It's certainly true that those types of changes were made, but these rules are must broader than simply that. There really are extensive changes to [the rules] and nearly all of them are welcome from my perspective as alleviating regulatory burden."

The changes to Stark are especially important because it is easy to fall out of compliance with the complicated law. "Stark has always been a morass of definitions within definitions, cross-references to other cross-references and broad pronouncements in what is supposed to be a bright-line, strict liability rule," Mikel notes.

If an arrangement does not follow the law to the letter the parties are in violation, even if they were unaware that they were not in compliance. That means they could face "recoupment, triple damages per claim, False Claims Act exposure and return and refund obligations for known overpayments. The update gets rid of some of the ambiguities," Mikel says.

New rules open paths to new arrangements

Practices and physicians may be able to enter into a variety of new agreements next year, thanks to the new rules. Here are a few examples:

1. **The new cybersecurity exception** under Stark and Anti-Kickback Statute safe harbor allow a provider such as a hospital to donate cybersecurity items and services to physician practices, Lovitch says. "And it could be software or hardware, which is really important because the current electronic health records exception and safe harbor does not cover hardware," and many medical practices may not have the resources to get the software or hardware themselves," Lovitch notes.
2. **The limited remuneration exception** allows "limited remuneration to be paid to a physician even though the practice and provider making payment don't have a written agreement in place," Lovitch says. Under the new exception at 411.357(z) organizations can pay up to $5,000 for certain services performed by the physician or people acting on the physician's behalf, Lovitch says and gives the example of a hospital that needs call coverage or medical director coverage due to the unexpected departure of a physician. To fill the gap "the parties quickly

agree that they'll pay $100 an hour for a week or two weeks and they don't get a written agreement right away." Under the current law there's no exception that would cover this arrangement.

3. **If a physician practice enters into an independent contractor arrangement** with a hospital, there is a new 90-day grace period for memorializing the agreement," but the parties will still need to agree to the compensation before the agreement's start date, Smith says.
4. **Commercially reasonable arrangements** don't have to be profitable to comply with Stark, Mikel notes. "There were a number of hospitals that in evaluating whether they could employ and pay a physician," determined that they would end up incurring a loss based on what they would have to pay the doctors. "So the thought process was that it can't be commercially reasonable because it's not commercially reasonable to take a loss." Now the definition explicitly says it is not based on whether the arrangement is profitable, Mikel says. "That really makes a lot of sense and meshes with reality. Some specialties don't get reimbursed as much but they're integral to a comprehensive care model."

Review current arrangements now

Based on the initial analysis of the laws, health care compliance experts say that in most cases an arrangement that fits an exception or safe harbor now will be compliant under the changes that go into effect next year. However, the changes to the definition of fair market value, commercial reasonableness, real estate contracts, equipment leases and other key terms, make it worthwhile to review contracts to see if they need to be tweaked, Mikel says.

If your practice is part of an ACO or similar coordinated care arrangement that complies with current laws, you should review the arrangement to make sure it will meet the new value-based exceptions and safe harbors and determine if you will need to make changes, Morgan says.

Changes to the Anti-Kickback Statute "might cause some parties to look at existing arrangements that didn't fit a safe harbor previously," but went ahead based on risk analysis, Aiken-Shaban says.

More steps for 2021

"As we move into the new year parties tend to look for new partnerships, [practices] will want to look at these rules" and potentially take advantage of the new flexibilities, Aiken-Shaban says.

Take the time to study the various new and revised exceptions and safe harbors, Lovitch says.

For example, the new cybersecurity exceptions and safe harbors allow donations of hardware, but it must be dedicated to protecting data and it can't be multifunctional. That excludes computers or laptops or any other device that can be used for a variety of tasks, says Rachel Yount, associate attorney, Mintz, Washington, D.C.

In addition, "all of the value-based exceptions have a lot of onerous requirements, a lot of documentation requirements, disclosure requirements, requirements for governing bodies," Yount says.

Practices should also note that the OIG restated its long-standing concern that physician-owned distributorships (POD) "are suspect and went out of its way to exclude them," Yount says. So make sure your POD or related supplies and services are not involved in the deal.

Finally, practices should watch the new administration for tweaks to the new rules. "Because of the timing of the publication, it remains to be seen what the Biden administration will do with these rules," Aiken-Shaban says.

"For the rules that are set to go into effect on January 19, 2021, for administrative procedural reasons, it is possible that the Biden administration could issue a hold on the regulations," Morgan says.

Health care attorneys say it is unlikely the new administration will eliminate the rule, but it might delay the effective date. For this reason, if you're going to start a new arrangement "don't make your effective date January 20," Aiken-Shaban says. ■

RESOURCES:

Stark update fact sheet: www.cms.gov/newsroom/fact-sheets/modernizing-and-clarifying-physician-self-referral-regulations-final-rule-cms-1720-f

Medicare Program; Modernizing and Clarifying the Physician Self-Referral Regulations public inspection version: www.federalregister.gov/public-inspection/2020-26140/medicare-program-modernizing-and-clarifying-the-physician-self-referral-regulations

Anti-kickback update fact sheet: https://oig.hhs.gov/reports-and-publications/federal-register-notices/factsheet-rule-beneficiary-inducements.pdf

Revisions to the Safe Harbors Under the Anti-Kickback Statute and Civil Monetary Penalty Rules Regarding Beneficiary Inducements (public inspection version): www.federalregister.gov/public-inspection/2020-26072/medicare-and-state-health-care-programs-fraud-and-abuse-revisions-to-safe-harbors-under-the

CMS

Prepare for expansion of Open Payments reporting to NPPs

By Marla Durben Hirsch

It's time to revisit your practice's relationships with applicable organizations. Starting Jan. 1, 2021, they'll be required to track and report payments to non-physician practitioners (NPPs) and report the information to CMS starting in 2022 *(MPCA 3/2020)*.

The Open Payments program, established by the Affordable Care Act, is a data aggregation and reporting system that promotes more transparency in health care by making the financial relationships between providers and drug manufacturers, device manufacturers, and group purchasing organizations (GPO) available to the public. Manufactures and GPOs must report payments or other "transfers of value" of $10 or more. These include gifts, consulting fees, research activities, food, speaker fees, education, and entertainment.

"It's based on the premise that relationships need to be scrutinized where there's an exchange of value because of [the potential] conflict of interest. It's tied to the concern that payments are made to influence referrals in violation of the Anti-Kickback Statute," says Edward Buthusiem, managing director in the Berkeley Research Group's health analytics practice in Philadelphia.

"There's a legitimate need for periodic training, education, etcetera. But within that there's a cadre of things that cross the line," he adds.

Under the current rules payments to NPPs do not have to be reported and this creates a loophole, because a manufacturer or GPO can give a gift to an NPP who works for a physician. This makes the NPP a conduit to the physician, says Buthusiem.

NPPs are also a major force in the provision of health care. They often have prescriptive authority and purchasing power. Some have their own offices. They also provide consulting services and training on behalf of manufacturers, according to attorney Judith Waltz, with Foley & Lardner LLP in San Francisco.

"They're stepping in for doctors. Why shouldn't they be subject to the same transparency rules?" she says.

The six new provider types that will be added to the list of providers whose transfers of value will be collected and reported are:

1. Physician assistants.
2. Nurse practitioners.
3. Clinical nurse specialists.
4. Certified registered nurse anesthetists.
5. Anesthesiologist assistants.
6. Certified nurse-midwives.

"Before sales reps would see physician assistants and nurse practitioners [over a free lunch] because those meals would not be reportable. Now assume that it's all reportable," Buthusiem says.

4 tips to handle the expansion

1. **Take a hard look at how the practice engages with manufacturers and GPOs.** Avoid an agreement that invites unwanted scrutiny, says Buthusiem. It's one thing to receive a small honorarium for conducting an education presentation; it's another to receive a lucrative speaker deal where there's little substantive information is presented. "If it sounds too good to be true there's probably an expectation [of referrals] with it," says Waltz.
2. **Have an internal system to monitor these relationships.** If anyone has arrangements that are subject to the Open Payments program, make sure that someone in the practice is approving and tracking them, says Waltz. That will help ensure that they are above board. Also, if you later disagree with what's been reported you have documentation to refute the information.
3. **Review the data of all providers subject to the Open Payments program each year.** "You need to be aware of the numbers reported on you," says David Zetter, president of Zetter Healthcare Management Consultants in Mechanicsburg, Pa. Practices can register to review their data on the Open Payments website.
4. **Dispute reported payments that you believe are incorrect as soon as possible.** Providers can dispute data that has been published any time during the year it has been reported. However, since manufacturers need to report by March of each year, it's best to review the reports in April or May so that if something is incorrect you can dispute it in sufficient time for the company to correct it before the data is

published on the website June 30. Otherwise it can be corrected but it's still publicly available. ■

RESOURCES:

Open Payments Program: www.cms.gov/OpenPayments

Types of payments reported: www.cms.gov/OpenPayments/About/Natures-of-Payment

Billing & coding compliance

Consider adding remote patient monitoring to your practice

By Marla Durben Hirsch

Practices looking for a way to improve patient care and boost the practice's income may want to look into — or increase their use of — remote patient monitoring, also known as remote physiologic monitoring.

Remote patient monitoring is the use of a device that collects patient data and transmits it to a clinician or monitoring entity wirelessly via the internet so that the clinician can evaluate the data and take action when needed. A myriad of information can be monitored remotely, including a patient's blood pressure, heart rate, and weight.

Remote patient monitoring has been found to improve patient outcomes, enhance the continuity of care, improve patient lifestyles and increase access to care, according to Richard Romero, senior vice president of the Coker Group in Brentwood, Tenn., speaking at the Physician-Legal Institute's Health Care Delivery and Innovation Virtual Conference in September.

It's also covered by many insurers, including some private payers, Medicare, and 23 Medicaid programs. In addition, 13 states mandate coverage for it. "These numbers are expected to increase," says attorney Rachel Goodman, with Foley & Lardner in Tampa, Fla., also speaking at the conference.

Moreover, Medicare's restrictive telehealth rules, such as originating site restrictions and interactive audio/visual equipment, don't apply to remote patient monitoring, so it may be easier to add it to a practice without much outlay. "Medicare pays for remote patient monitoring under the same conditions as in-person physician services," says Goodman.

Remote care is on the rise

The COVID-19 pandemic, which increased the need for contactless care, combined with technological innovations in the devices have spurred the use of remote patient monitoring this year.

According to the Medical Group Management Association (MGMA), the number of physicians that have incorporated remote patient monitoring into their practices has increased from 6% in 2017 to 21% in 2020.

CMS changed Medicare's rules in response to the pandemic in March, allowing remote patient monitoring for both chronic and acute conditions, and to new patients as well as established ones. Similarly, the Food and Drug Administration issued emergency use authorizations for certain devices to help increase the availability of remote treatment during the pandemic. These steps have made it more feasible for practices to add or increase these services.

"We're seeing an acceleration in remote patient monitoring that no one could have predicted," says Goodman.

Rules that soften the fraud and abuse laws would enable providers to offer more free equipment to patients, opening the door for further remote patient monitoring (*see story, p. 1*).

Remote patient monitoring does come with some challenges. For instance, there needs to be reliable connectivity and transmission capability to obtain and use the data. This can be problematic in areas with inconsistent Wi-Fi. The data also needs to be integrated into a physician's electronic health record, says Romero.

Additionally, some logistics issues will need to be ironed out. Very few physicians build their own remote monitoring platform, so most work with a third-party vendor for the technology. Many practices also contract for some services provided by the vendor, such as data collection. This raises operational questions as to how and to what extent a practice wants to offer this service and how to incorporate it into the workflow.

"[The practice needs to determine] who will do the patient engagement and education, the device management and the data monitoring," says Romero.

Still, these are not necessarily barriers for those who want to jump on this bandwagon.

"[This service] is the next wave," he says. ■

RESOURCES:

MGMA statistics on remote patient monitoring: www.mgma.com/data/data-stories/practical-steps-for-remote-patient-monitoring-serv

FDA expansion of authorized remote patient monitoring devices: www.fda.gov/medical-devices/coronavirus-disease-2019-covid-19-emergency-use-authorizations-medical-devices/remote-or-wearable-patient-monitoring-devices-euas

Billing & coding compliance

10 compliance areas that impact remote patient monitoring

By Marla Durben Hirsch

Incorporating remote patient monitoring into a physician practice can improve patient care and boost a practice's revenue stream (*see story, p. 5*).

"It's an opportunity and exciting. Telehealth and remote patient monitoring are redefining how to deliver health care. It's a different world," said attorney Rachel Goodman, with Foley & Lardner in Tampa, Fla., speaking at the Physician-Legal Institute's Health Care Delivery and Innovation Virtual Conference in September.

However, remote patient monitoring brings its own set of compliance issues that can trip up the unwary. These include:

- **Device selection.** The device must be approved by the Food and Drug Administration and capture physiologic data. Practices also need to choose carefully which device and vendor to work with, since the data needs to be reliable and valid, said Richard Romero, senior vice president of the Coker Group in Brentwood, Tenn., also speaking at the conference.
- **Billing snafus.** There are five main CPT codes for remote patient monitoring, but the rules for them vary and can be confusing. For instance, the analysis and interpretation of data code (**99091**) can only be rendered by a physician or other qualified health care practitioner, and Medicare requires direct supervision of staff. Collection of data (**99453-99454**) must be ordered by a qualified practitioner, but the services can be performed by staff, including a vendor's staff, said Goodman. Those codes, as well as management of treatment (**99457-99458**) allow for general supervision.
- **HIPAA.** While a vendor providing services would have access to individual patient records as a business associate, practices don't want to grant vendors wholescale access to their medical records, since that could violate HIPAA's security and privacy restrictions *(MPCA 7/2018*). "A vendor should not be going through your records to determine who should get remote patient monitoring," says Goodman.
- **Fraud and abuse.** Since remote patient monitoring typically requires the use of a third-party vendor, the deal needs to be at fair market value to avoid kickback allegations. "[One can't] get too great of a deal," warns Romero. The fraud and abuse laws can also be implicated if the provider isn't sufficiently involved, since the services need to be ordered by a qualified clinician. "It can't be a turnkey arrangement [with a vendor]. You need skin in the game," says Goodman. There can also be medical necessity issues. "Make individual assessments. Don't do remote patient monitoring with all patients with a particular condition," warns Goodman.
- **State laws.** Some states have different requirements for remote patient monitoring that need to be followed. For instance, providers typically need to be in the state where the patient is located, and the scope of practice laws may require direct supervision even where Medicare requires only general supervision, says Goodman. Some states don't allow fee splitting between the physician and the vendor, so you may not be able to have the vendor market on your behalf.
- **Device logistics.** The practice will need to determine whether the device can be remotely adjusted and whether the vendor should set automatic critical and panic alerts, says Romero. Other operational questions include how devices will be cleaned and collected, and whether, depending on the device, patients get to keep them.
- **Education.** Staff will need to be properly trained about how to perform the data analytics, and patients may need to be trained in how to handle the equipment, says Romero. Billers will need to learn how to bill and code for the services. Any contracted staff from a vendor will also need to be included in any training, such as HIPAA compliance.
- **Accountability.** While a vendor may be performing much of the services, the practice is still on the hook for clinical or other issues. "Don't lose sight of the fact that even if you hire a remote monitoring vendor, you're responsible. It's done under your supervision," says Goodman.
- **Patient cost sharing.** Patients may be on the hook for a portion of the cost. For instance, Medicare requires patients to pay 20%. However, since the patient usually won't be in the office when receiving the service, the practice won't be able to collect the patient cost sharing at the time of service and will need an alternative method to obtain these payments, says Goodman.
- **Malpractice liability.** Remote patient monitoring raises questions about the standard of care and product liability. "Talk to your malpractice insurer to make sure you have appropriate coverage," says Goodman. ■

Privacy & security

3 steps to add evolving HIPAA areas to HIPAA training

By Marla Durben Hirsch

All covered entities need to periodically train their workforce on HIPAA compliance. But if you're using older training tools, your training may not be up to date (*MPCA 10/2020*). To ensure that newer and evolving areas are included in employee HIPAA training, consider these steps:

1. **Review your current HIPAA policies and procedures and see what's missing.** "They should be the basis for your training," says attorney Elizabeth Litten, with Fox Rothschild in Princeton, N.J. If you identify gaps, update your policies and procedures accordingly. For instance, if you added a new patient portal, make sure that's added to your policies and procedures on HIPAA compliance and that staff knows how to keep the data in it secure. says Litten.
2. **Make sure that the training occurs.** "If you don't it's communicating [to staff and others] that it's not important, and that can come back to bite," says attorney Michael Kline, also with Fox Rothschild in Princeton. Note that HIPAA is flexible about training. It doesn't dictate how often or in what way a provider conducts the training, only that it be provided to new workforce members and to everyone on a periodic basis. It also doesn't need to be in-person. There are resources online, many of them available for free from associations and other sources. The HHS Office for Civil Rights (OCR) also offers HIPAA training tools on its website. Physicians can receive free continuing medical education credits for training about patient access to their health records.
3. **Document that everyone in the practice has been trained.** It's not only a compliance requirement; it also reduces the risk that a privacy or security violation will occur. Training is one of the HIPAA compliance issues the OCR looks into during a HIPAA investigation "[Evidence of training] is like an insurance policy. OCR will be asking," says Litten. ■

RESOURCE:

HIPAA training materials: www.hhs.gov/hipaa/for-professionals/training/index.html

Privacy & security

Ransomware rising: Protect WFH, telehealth; update your IT plan

By Roy Edroso

Ransomware, a bane of health care providers for years, has gotten even worse, leading to steeper consequences for providers who have been hit by it. Adding to the challenges, the pandemic-induced wave of work-from-home (WFH) orders has made attacks easier for crooks. It's time to double down on your defenses.

On Oct. 28, HHS and the FBI, together with the U.S. Cybersecurity and Infrastructure Security Agency (CISA), announced in a joint report that they had "credible information of an increased and imminent cybercrime threat to U.S. hospitals and health care providers."

Cybercriminals have "continued to develop new functionality and tools, increasing the ease, speed and profitability of victimization" and increasingly aim it at the "Healthcare and Public Health Sector (HPH)... often leading to ransomware attacks, data theft and the disruption of health care services," the report states.

Ransomware is a kind of malware that began to emerge in the health care world in 2015. It is spread and launched by links in phishing emails opened by unwary employees and locks down connected computer systems; its operators demand payment, usually in cybercurrency such as bitcoin, to release the files.

By 2016, ransomware was so prevalent in health care that the HHS Office for Civil Rights (OCR) was obliged to rule on its HIPAA impact, announcing that unless the provider who was attacked could prove otherwise, ransomware attacks would be considered a reportable breach.

The latest offender

The impact has only increased in recent years, and in response HHS laid out "Voluntary Cybersecurity Practices" with which practices might defend against it in 2019. The current report warns providers that a major cybercriminal enterprise called TrickBot "now provides its operators a full suite of tools to conduct a myriad of illegal cyber activities," among them the recent ransomware varieties Ryuk and Conti.

Virtual private network company NordVPN reports that Ryuk is "believed to be behind the recent ransomware attack on Universal Health Services (UHS), running

approximately 400 hospitals and care centers across the United States and the United Kingdom, making it one of the largest medical cyberattacks in U.S. history."

And it's not just hospitals that have to worry.

"While hospitals, due to their sheer volume, are larger treasure troves of information, often independent physician practices could be tempting targets because most don't have large dedicated IT departments to focus on cybersecurity protections for the practice," cautions Rich Temple, vice president and CIO at Deborah Heart and Lung Center in Brown Mills, N.J.

Health care faces heightened risk

Ransomware is booming because it's a quick way to make money — sometimes lots of it.

"I have seen demands for ransoms rise tenfold in 2020," says Oli Thordarson, CEO and founder of Alvaka Networks in Irvine, Calif. "I saw my first $20M ransom last month."

Also, ransomware has been "commodified" — that is, it's sufficiently mature that successful hackers are selling kits on the Dark Web so others can use it, according to Sue C. Friedberg, co-chair of the Cybersecurity and Data Privacy Group at Buchanan, Ingersoll & Rooney in Pittsburgh. Ultimately, that means there are more criminal entrants in the market.

But also ransomware has gotten more intense, and hackers are able to extract data more aggressively than before, says Kristen Dauphinais, head of U.S. cyber and technology with Beazley in Dallas.

"When we really started seeing ransomware events in earnest, they were very simple, kind of smash-and-grab jobs," Dauphinais says. "You'd have somebody click on a link that would allow the malware into the system, and the files would be encrypted."

But now, "it's become much more complicated and invasive," Dauphinais says. "Ransomware is getting into the system, but the bad actors are sitting in that system and waiting much longer to act. Meanwhile they're watching traffic to see how people communicate there and where information systems are and aren't protected, in addition to getting the malware onto the backups."

This allows the crooks to feel their way around the system, find data they might not have bothered to seek out before, and exfiltrate, or extract, it before finally announcing the lockdown of the victim's entire system.

"We are now seeing situations where the ransomware may actually be a parting gift, if you will, after other access and activity in the system," says Pamela E. Hepp, a shareholder and the other co-chair of the Cybersecurity and Data Privacy Group at Buchanan, Ingersoll & Rooney. "And they may have been there for a period of time, but had not been detected until the ransomware attack. In some respects, the ransomware attack may be intended to hide their tracks, and when you get in and do the analysis, you realize that it was a parting gift."

The exfiltrated medical and personal data can be very valuable to thieves. For example, it enables medical identity theft, which "allows a fraudulent person to receive healthcare benefits they're not entitled to, as well as access to prescription history," says Steve Tcherchian, chief information security officer at cybersecurity analytics company XYPRO in Simi Valley, Calif. "This enables thieves to purchase prescription drugs on a patient's behalf, which are then resold online on black market websites."

Also, hackers may separately ransom sensitive personal data skimmed in the attack and threaten to "post the data or make it available either for sale or just to make it available, as an embarrassment to the entity," Friedberg says.

Where the problems lie

Experts agree that the pandemic-inspired WFH and telehealth trends have left medical entities more vulnerable, as home workers on laptops and providers interfacing with patients on Skype improvise their own approaches to security, relatively unmediated by their company's IT department.

"The shift to WFH was sudden and unplanned by most firms," Thordarson says. "The IT teams, and even some contractors, were not adequately staffed with the right skills to do this properly and securely."

Slackened security on telehealth since OCR allowed providers to use non-HIPAA-compliant software and devices has also amplified insecurities.

CISA issued a ransomware guide in September listing protocols it recommends for defense. Many are technical in nature — for example, to discourage phishing they suggest "disabling macro scripts for Microsoft Office files transmitted via email." (**Note:** Administrators can do this via the Microsoft "Trust Center" feature.) Some are precautions you've probably been hearing for years, e.g., "If you are using passwords, use strong passwords É and do not reuse passwords for multiple accounts."

Insurers and other service companies in the cyber space can talk you through appropriate defenses. Beazley, for example, gives prospective clients of their ransomware-related services a questionnaire, developed by them in conjunction with Lodestone Security and KPMG, with questions about email security (e.g. "How often is phishing training conducted to all staff [e.g. monthly, quarterly, annually]?"), internal cybersecurity (e.g., "Do your users have local admin rights on their laptop/desktop?"), and backup and recovery policies (e.g., "Are you able to test the integrity of back-ups prior to restoration to be confident it is free from malware?").

"Every underwriting question verifies the existence of a protocol or procedure that will stop an event in its tracks," Dauphinais says. "We want our clients to be thinking about a holistic infrastructure designed to quarantine any such event should it occur."

Other experts repeat the usual cautions. "All the basics have to be followed," Friedberg says. That includes "making sure access credentials are changed regularly, multifactor authentication [and] limiting the number of people who have administrative privileges to a system." Also, use patches as soon as your tech vendors announce them and VPNs for any offsite work. "It's just that much more significant when people are operating from their own home systems," Friedberg says.

Experts also say you need to act now. "We've been saying for years that you can't put that off to next year or put it in next year's budget — you've got to do it now," Hepp urges.

3 tips to protect yourself

1. **Segregate backups.** Since hackers are reaching deep into your systems, now's the time to get serious about doing backups they can't reach, offline or on the cloud. "Set aside a nightly copy of your backups in such a way that even if your IT team wanted to delete backups, they could not unless they were physically in the room with the backups," advises Nathan Little, senior vice president of digital forensics and incident response for Tetra Defense in Madison, Wisc. Try to fix it so that as little as possible of your data is available to hackers at any given time.
2. **Get aggressive on email.** You might resort to whitelisting protocols that block certain kinds of traffic, though there's always an efficiency tradeoff there. Temple notes there are "hash hunting" programs that can identify URLs or file "hashes" — an encrypted value that is extracted from the contents of a file or message — in emailed files and block the ones they have reason to believe are malicious. Training staff remains the best line of defense, but you can step that up, too. "Phishing [vulnerability] is a really easy thing to test with fake emails to see who clicks and who doesn't," Dauphinais says.
3. **Get help.** Don't have the IT bandwidth for the job? Call for backup. "Many organizations have popped up in the past year to help providers monitor aberrant activity both at their network firewalls as well as on different computer assets within their network," Temple says. These companies include vendors of "remote network monitoring, risk modeling, rapid incident response and assistance with disaster recovery and business continuity." ■

RESOURCES

HHS, FBI, and CISA: "Alert (AA20-302A), Ransomware Activity Targeting the Healthcare and Public Health Sector," Oct. 28: https://us-cert.cisa.gov/ncas/alerts/aa20-302a

CISA Ransomware guide, Sept. 2020: https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

Simplify Compliance
Learn, Comply, Succeed

SUBSCRIBER INFORMATION

Have questions on a story? Call or e-mail us.
1-855-CALL-DH1

***MEDICAL PRACTICE COMPLIANCE ALERT* TEAM**

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

Marla Durben Hirsch, x6015
Content specialist
mdurbenhirsch@decisionhealth.com

Julia Kyles, CPC, x6015
jkyles@decisionhealth.com

Medical Practice & Hospital community!
www.facebook.com/DecisionHealthMP
www.twitter.com/DH_MedPractice
www.linkedin.com/groups/4048762

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

REVENUE CYCLE FORUM
To join the free medical practice revenue cycle forum, our free Internet forum for revenue cycle specialists, including compliance managers and auditors, go to *http://practiceforum.decisionhealth.com/* and register.

Medical Practice Compliance Alert® is a registered trademark of DecisionHealth. *Medical Practice Compliance Alert* is published 12 times/year by DecisionHealth, 100 Winners Circle, Suite 300, Brentwood, TN 37027. ISSN 1047-1863. *www.decisionhealth.com* Price: $547/year.

Audit adviser

Don't let prolonged service changes trigger denials in 2021

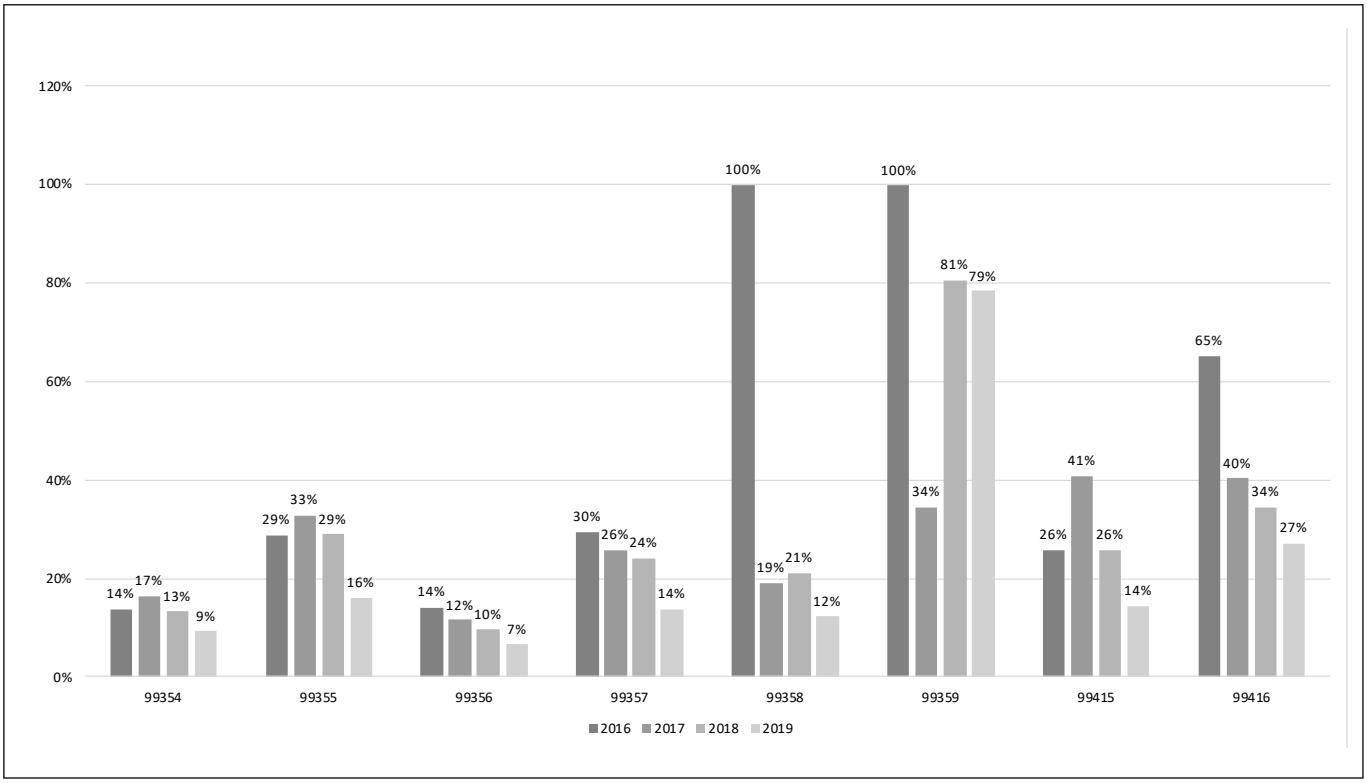
By Julia Kyles, CPC

The new prolonged service code that can be reported with office visits next year (**99417**) is getting a lot of attention, but pay attention to the changes to the rest of the code family that will go into effect Jan. 1, 2021, and watch for a spike in denials.

This month's chart shows that denials are an ongoing problem for these codes and many of the pending changes will make it easy for a Medicare administrative contractor (MAC) to spot practices that aren't using the new guidelines. Two of the biggest flags will be attempts to report prolonged outpatient service codes **99354-99355** or non-face-to-face codes **99358-99359** in conjunction with an E/M office visit (**99202-99215**). The outpatient codes can't be reported with office visits next year according to the 2021 CPT Manual and Medicare will halt coverage of the non-face-to-face codes when they are connected to an office visit. Practices should note that if the MAC accidentally pays for the non-covered service, they must return the money.

Finally, check the medically unlikely edits (MUE) for codes associated with additional prolonged time: 99355 and **99357** for inpatient and observation services and **99416** for clinical staff services. MUEs are updated quarterly and claims that exceed the daily limits are another sign a practice isn't keeping an eye on guidelines.

Prolonged service denials, 2016-2019



Source: Medicare Part B utilization data