EISNERAMPER

Practice Strategies

A Newsletter for Healthcare Professionals

Spring 2016

A Matter of Leverage

How Mid-Levels Can Transform Your Practice

The role of mid-level providers — nurse practitioners, physician's assistants and other advanced clinical providers — is expanding in our ever-evolving healthcare system.

Thanks to the Affordable Care Act and an aging population, more Americans are seeking health care. At the same time, payment models are increasingly rewarding quality over quantity. Practices most likely to succeed in this era of accountable care have figured out ways to leverage mid-level providers to not just handle increased patient volume, but also provide better outcomes.

Improving Productivity and Access

In the primary care setting in particular, overburdened physicians are utilizing mid-levels to bolster productivity and patient access while also providing the patient education and follow up that help prevent complications and re-admissions. Here's how it typically plays out:

Main Street Family Practice brings a nurse practitioner onboard who can treat upward of 80 percent of the patients seen each day. The remaining 20 percent of higher acuity cases are referred to one of the practice's physicians. Medicare and private insurers reimburse the new nurse practitioner at anywhere from 80 percent to 100 percent of what Main Street's physician providers receive.

With a mid-level handling the typical colds and sprains, the physicians are free to concentrate on more complex, higher-reimbursing cases. At the same time, the physicians are able to spend more time with patients, even while supervising the work of nurse practitioners.

It's not just general and family practice physicians who are benefitting from using mid-levels. Specialty practices are incorporating physician assistants and nurse practitioners into the mix to reduce wait times for specialty services. In particular, specialties such as pediatric, women's health, psych/mental health and gerontology are leading the pack.

Three Ways It Could Work

Of course, you'll need to take into consideration the scope of practice laws for mid-levels in your state (many states are currently considering expanding the scope of practice for nurse practitioners). In general, there appear to be three key roles that mid-levels are well-suited to play.

1. Handle acute care visits — A PA or NP can be utilized to improve same-day patient access and extend practice hours for acute care visits. This is perhaps the easiest way to quickly incorporate a new mid-level.

2. Become a member of an integrated care team — A mid-level can

Continued on page 3

Data Security

Protecting Patient Data Is *Your* Responsibility

There was a time when a locked file cabinet was all that was needed for "data protection." Today, the profusion of digital data at the practice level requires a much more involved and vigilant approach.

Small medical practices — just like small businesses and mom-and-pop retailers — are particularly appealing targets to data thieves trolling for Social Security numbers and credit card information. These practices often lack the advanced technology to deter attacks and typically do not have dedicated IT staff keeping a watchful eye.

The Stakes Are High

Unfortunately, patient privacy laws cut providers no slack. HIPAA legislation pins the blame for data breaches squarely on "covered entities" — doctor's offices, health insurers and hospitals. Fines can range from $100 to $50,000 per violation, with maximum fines reaching $1.5 million in cases where willful neglect can be proven as a cause for the breach.

Furthermore, the HITECH Act requires that patients affected by a data breach be notified and that any data breach involving more than 500 patients be reported to that state's media outlets. Obviously, any breach that is made public could have a serious impact on your reputation.

Set a Watchman

The reality is that medical practices need to act as their own watchdogs and protect their patients and themselves from the dangers of a data breach. Consider these key steps for protecting patient data:

Create a culture of data security. If there is no dedicated data security team, data security must become the job of everyone in the practice. Create a formal data protection policy and provide continuous training on security best practices. Also create an incident response plan that outlines the steps to take (and who will take them) in the event of a data breach. Here, you can turn to a third-party contractor for help.

Guides to developing data security policies and procedures are available from the American Medical Association, the American Academy of Family Physicians and the American Dental Association. Finally, give your policies some teeth by establishing consequences for violations (e.g., verbal/written warnings, unpaid suspensions, termination).

Develop a data retention plan. Obviously, the less data flowing through the pipes, the less likely the chance of springing a leak. A basic data retention policy that outlines what data should be kept, where it should be stored and for how long can help ensure that you don't keep more data than needed.

Put someone in charge. HIPAA requires practices to name a security officer as the point person for implementing data security regulations. Assign security to one person — preferably someone with real authority, such as a doctor or office supervisor — and give him or her the resources and time to do the job. This may include conducting a risk analysis, creating procedures and policies, training employees, and ensuring that all computers are kept up to date with security patches.

Encrypt appropriately. Under the HITECH Act, loss of encrypted data is not considered to be a data breach. Make sure all back-up hard drives, the network and any hardware (laptops, flash drives, smart phones, etc.) are encrypted to at least 178 bits.

Control access. Consider giving administrators login and authentication on computers and networks at your practice, including controlling access and validating privileges.

Assess risk. Utilize the free HIPAA Security Risk Assessment Tool to ensure compliance with HIPAA's administrative, physical and technical safeguards.

Ultimately, digital data is a boon for improving healthcare delivery. But it certainly ups the ante for hackers and thieves to steal valuable personal information — making data security critical for your practice. ■

Data Breaches That Made the News

It's not just Target and the IRS that are getting hacked these days. Healthcare providers of all sizes are experiencing data breaches, including these:

Hollywood Presbyterian Medical Center in Los Angeles agreed to pay the equivalent of $17,000 in bitcoins to regain control of its computer systems after the facility was hacked in a "ransomware" attack.

Former employees allegedly breached data systems at an Owensboro, Ky., medical group, stealing information from about 3,000 patients to start their own business.

Radiology Regional Center, PA, in Fort Myers, Fla., was forced to notify patients of a data breach when paper records containing personal information were accidentally "released" by its records disposal vender while en route to the destruction facility.

The Role of Mid-Level Providers

Continued from page 1

function as an extension of the primary care physician on a care team. He or she would handle lower-acuity visits and provide chronic and preventive care as well as treatment of acute problems. Physician productivity can be expected to benefit from this approach.

3. Operate as a fully paneled provider — A nurse practitioner could also be given full responsibility for an entire patient population. Depending on state laws, this approach may allow for the largest degree of patient panel expansion at a lower cost than hiring an additional physician.

Of course, patients would need to be educated about the capabilities of mid-level providers to ensure they are comfortable seeing one as their main primary care provider.

Do the Math

Mid-level providers are able to perform about 80 percent of a primary care physician's work while collecting about 70 percent as much in revenue. In 2015, the mean full-time base salary for mid-level providers was $97,083. This means mid-levels can bring in more revenue in proportion to their compensation than most internists and family physicians.

In fact, for every $1 in compensation, the typical PA brings in $3 in gross earnings for the practice, according to the Medical Group Management Association. By contrast, internists typically gross slightly more than twice their compensation.

Integrate Them Properly

Educate your office staff and billers on the laws and specifications of any non-physician providers so they fully understand the mid-level's role, capabilities and impact on practice workflow and patient service. Likewise, take the time to introduce mid-levels to patients as colleagues. Make sure patients understand that you will always be available should they desire to "see the doctor."

Finally, remember that successful practices treat mid-levels as healthcare providers, not employees. Their pay is incentive-based (i.e., a competitive base salary with financial incentives around volume, quality outcomes, cost containment, etc.).

The competition for mid-levels will certainly heat up under healthcare reform as busy waiting rooms and an emphasis on primary care increase demand for these "extenders." With that in mind, physicians are well-advised to make sure they are offering the right combination of salary, benefits and work-life balance to retain existing NPs and PAs — or recruit new ones. ■

Contact our office for help "running the numbers" and determining if a mid-level provider makes sense for your practice.

Are You Ready for a Mid-Level?

Your practice might be ready for a mid-level if:

The practice has grown to the point that same-day appointment slots have all but disappeared and new patients are being turned away.

You're seeing more patients than you'd prefer or finding that your established patients need more care than you can comfortably provide.

You're a mid-career doctor looking to reinvigorate your professional life by focusing on more challenging cases or developing expertise in a new area.

In any of these cases, you may be willing to exchange a short-term drop in income for a less-harried patient load.

The Telltale Signs of Fraud

Fraud comes in many shapes and sizes, but the telltale signs of employee theft are fairly consistent. In particular, physicians and practice managers should be on the lookout for the following signs:

1. Unusual entries: A perpetrator enters a credit, which is then used to reduce recorded cash to reconcile with the cash on hand after a theft. Or, a credit is used to set up an account payable for a fake entity that the perpetrator will eventually cut a check to.

Action: Randomly audit journal entries to determine their legitimacy.

2. Suspicious vendor invoices: Of particular concern are vendors who always insist on dealing with the same accounting or administrative staff, as well as transactions in which the same person authorizes the purchase, approves the vendor invoice and makes the payment.

Action: Have a practice partner or office manager compare original vendor invoices, purchase orders and receiving reports. Also review cancelled checks. Legitimate vendors deposit checks into their business accounts — they don't cash them or deposit them into a personal account.

3. Forged receipts: Co-payments are collected at the time of service but are not recorded to the patient's accounts. The charge is later written off as an adjustment to the patient receivable.

Action: Reconcile deposits to patient records daily.

4. Diverted collections: Patient or third-party payments are diverted to a personal bank account and the patient receivable is written off as an adjustment. This scam typically shows itself when patients start calling regarding overcharging and inconsistencies in their billing.

Action: Verify adjustments to the explanation of benefits or chart documentation.

In the end, establishing good internal controls is a vital defense against fraud. And it typically requires an investment of as much attention as money. ■

Contact our office today for help evaluating your internal controls.