Keeping Compliant: Managing Rising Risk in Physician Practices

Save to myBoK

By Lori Brocato, Steven Emery, and Jan McDavid, Esq.

A mix of new regulations and initiatives-with audits and attestations in their wake-have put a new focus on compliance in physician practices and clinics.

Recovery audits, breach notification regulations, and modifications to the HIPAA privacy rule are forcing rapid workflow changes within healthcare organizations and mandating a new level of awareness and planning to maintain both compliance and productivity. Much of the discussion on these topics has related to the acute care hospital setting. Less attention has been paid to physician or group practices and clinics.

While the requirements are largely similar in both settings, practices and clinics face unique challenges in meeting them, particularly a lack of staffing and resources dedicated to compliance. They must bring a new focus to compliance, identifying cost-effective ways to successfully manage the changes, including staffing, processes, and technology.

Few Staff to Manage Many Changes

Perhaps the biggest difference between the hospital and practice settings is the scale of operation. Many practices have limited financial and human resources to deal with increased volumes, technological advances, or workflow changes.

The shortage of skilled workers, specifically in the areas of claims audits and security, is even more problematic in practices and clinics than in acute care hospitals. HIM skills are at a premium in small and mid-sized practices and clinics, and a limited number of staff must manage many responsibilities that often are managed by specialists in larger facilities.

The compliance or privacy officer in the average practice typically is also the practice administrator. The audit coordinator may also serve as resident billing and insurance expert, with little time to optimally manage audits and appeals. Release of information (ROI) often is done on a part-time or as-needed basis by office staff who juggle many other responsibilities. Unfortunately, this model of a single staff member supporting several specialized functions is becoming insufficient as the volume of work increases, the prevalence of recovery audits rises, and scrutiny on data security intensifies.

Additionally, these issues often require legal expertise typically not on a practice or clinic payroll. These changes are forcing the use of external, outsourced resources and consultants that increase the cost burden on these small businesses.

Increasing volumes and new risks are not the only challenges. Practices are also dealing with EHRs, meaningful use, HIPAA 5010, and ICD-10. In short, physician practices and clinics require a new mix of people, process, and technology to meet the ever-evolving healthcare landscape.

Managing Claims Audits Effectively

Experience to date shows that practices are getting hit hardest by Medicare Administrative Contractors (MACs)-specifically prepayment reviews-and there has also been a steady ramp-up in Recovery Audit Contractor (RAC) activity. The MAC audits are more onerous than the RACs because they are "pending claims" and withholding payments. There is no limit on the number of claims they can review, which can have serious financial implications for a physician practice.

To complicate matters, the majority of physician practices and clinics operate in a manual mode and use simple spreadsheets to track audit activity. As audit volumes increase, practices and clinics will require audit tracking and management software to keep up.

Electronic health record (EHR) systems will also help practices manage and minimize audit risk. Many EHRs have clinical decision support and health maintenance modules to stop improper billing of bundled procedures prior to billing, a common mistake caught by auditors. EHRs also monitor medically unlikely procedures and other billing edits. By catching potential billing problems early in the process, practices prevent future audits as well as identify new process and workflow changes.

Secondly, many audit issues are related to poor quality of clinical documentation. As in hospitals, clinical documentation improvement programs are critical in minimizing audit red flags and providing quick justification for medical necessity and reimbursement.

Finally, practices must ensure they avoid the common errors identified in current audit programs. This can be done online by determining which RAC target lists are also physician-based RAC problems. In addition, practices can reference resources such as the Medical Group Management Association, which provides information on audits. Diligent awareness, education, and auditor monitoring takes human resources, but it can pay for itself in fewer take-backs.

Common Audit Concerns

- Practice and hospital bill for the same service
- Improper bundling and unbundling of services
- Medically unlikely procedures
- Timed codes (e.g., services that can only be billed once a year)
- Injection billing that lacks documentation (e.g., for influenza)
- Mandated procedure combinations

Reducing Risk of Breach

The risk of data breach in physician practices varies greatly. Some practices have a considerable risk due to a lack of automation, education, and subject matter expertise on staff.

All healthcare providers have a professional obligation to safeguard the privacy and security of their patient data. Federal and state law imposes regulatory requirements and monetary penalties. Security lapses can result in fines, administrative costs, and more. Federal fines can reach $1.5 million for each patient whose data was breached. The average cost of breach in healthcare was $301 per patient in 2010, which included costs related to detection, investigation, notification, and possible services offered to affected individuals.[1]

Carelessness and forgetfulness are common causes of breach in practices and clinics. Most of the 30,521 "small" data breaches reported to the Office for Civil Rights in the 15-month period ending December 31, 2010 (breaches involving fewer than 500 individuals) resulted from clinical or claims records that had been sent to the wrong person.[2] Consistent, thorough education is central to reducing human error at the root of such mistakes.

Further breaches occur when medical records leave the office. Laptop computers pose a major risk. Encryption-at the drive-level, not the file level-is a simple step practices can take to better protect their patient information. HIPAA requires that data be secure both in transit and at rest. If electronic PHI is lost or stolen in an encrypted format, it is not considered a breach under federal regulation.

When it comes to security, an ounce of prevention is worth a pound of cure. Practices that invest in prevention reduce their exposure to breach. And if they do experience a breach, practices that can demonstrate they took reasonable steps to prevent unauthorized disclosures may receive reduced fines or perhaps avoid fines altogether.

Security efforts should include:

- Detailed security policies and procedures
- Regular staff training

- Ongoing internal audits
- A documented response plan for incidents
- Detailed risk assessments
- Detailed records of the facts surrounding disclosures, particularly the dates of events

The key is to know where patient information is stored and where it flows throughout the organization, whether it is in paper or electronic format. That understanding must then be applied to policies and procedures that are routinely taught and monitored.

This is not a situation where practices can write policy and procedure manuals and keep them on the shelf. They must be living documents, which are regularly updated and presented to staff in educational sessions.

Managing RAC Activity at Banner Medical Group

Banner Health is one of the largest health systems in the country. Headquartered in Phoenix, Arizona, with locations in seven states, Banner operates 23 hospitals and more than 100 physician offices and clinics. Leslie Morgan, CCS, HIMS audit program director, manages audit activity for the hospitals and the clinics. Morgan's biggest challenge is centralizing RAC request letters sent to practices and clinics and educating office staffs across such a large geographic area.

Demand letters for clinics go everywhere and to multiple practices. Centralized audit management, more easily accomplished in the hospital, is virtually impossible across hundreds of practices and clinics. Morgan focuses on building relationships with office staffs and educating them on the urgency of sending any RAC demand letters received directly to her attention.

Further, clinic demand letters contain very little information, making it difficult to interpret what the auditors want and if the denial is valid. Frequent visits to the Banner mainframe's database are required to backfill information.

Using a centralized audit management system, Morgan identified the top RAC issue for Banner clinics: evaluation and management (E&M) coding for new versus established patients. "Patients are considered new only if they were not seen by the same physician within the last three years," Morgan explains.

With more than 100 physicians at some clinics, separating new from existing patients by physician requires diligence and scrutiny. Registration clerks must carefully search for prior visits and correctly identify patient status. Common problems include:

- User error
- No history to determine if patient was seen previously
- Billing/provider number issue when multiple physicians use the same number

Once audited and verified as a recurring patient, Banner does rebill the case. This is a long manual process for very few dollars in recoupment. But with large volumes of RAC cases in this category the dollars add up.

The audit management system is used to log every request and manage the entire audit process. "Without the data you cannot see the trends and solve the underlying issues," Morgan says.

Tips for dealing with RAC audits in the physician practice or clinic setting include:

- Look at new versus established patients
- Capture audit data and report on denial/issue trends to identify source problems
- Create a process for managing audit letters and provide workflow for dealing with the different audit types
- Establish relationships with all clinic sites to facilitate process improvement and communication

Speeding Patient Access and Release of Information

HIPAA has required all covered entities account for disclosures of patient information since the privacy rule took effect in 2003. New proposed privacy rules resulting from the 2009 HITECH Act expand accounting of disclosures by requiring practices create access reports for electronic records.[3]

While these access reports would contain only a few basic facts for each entry, they must record every view, use, or disclosure of patient information within electronic health records, including the previously exempt uses for treatment, payment, and operations. As proposed, these reports must be available to patients on demand, and they must be consolidated from disparate systems and business associates into a single list.

Many organizations submitted comments in response to the proposed rule stating that the access report would be too burdensome and should be revised or abandoned. It remains to be seen which proposed provisions will be incorporated into the final rule.

Physician practices also must adapt their traditional release of information practices to stay compliant with industry changes. The meaningful use EHR incentive program, for example, requires workflow changes that may be felt more acutely in physician practices than in hospitals.

Meaningful use requires providers give patients electronic access to their records within three days of their request. This will force some practices to shift their ROI processing from a part-time or as-needed process to a daily function. Demonstrating meaningful use will benefit from robust ROI logging and reporting and tools rather than the paper logs still used in many practices. (These same tools offer other benefits, such as aiding in responding to audits by federal or state agencies.)

ROI under meaningful use gets more complicated when a patient sees multiple physicians, as is commonplace in large practices and clinic settings. If the patient requests an electronic copy of his or her information for a specific eligible professional (EP), then the practice must record the request and fulfillment related to that one EP. However, if the patient makes a request for an electronic copy of his or her information that is not related to a specific EP, the practice must record the request related to every EP with whom the patient has had a visit during the reporting period.

Producing the electronic copy or access within three business days will require many practices review and modify workflows and roles to ensure requests are properly received and logged. An inability to record and fulfill requests properly may cause a practice to fail its attestation on the measure and risk its eligibility to receive incentive payments.

Technology Becomes Essential

Practices and clinics have lagged hospitals in adopting health IT, managing their needs with paper processes. However, technology is becoming essential in the increasingly complex healthcare landscape. From the use of audit-tracking software to EHRs and electronic billing, technology presents a cost-effective solution to volume, productivity, and compliance concerns.

When evaluating IT products, practices should strive to make technology decisions that are good for the longer term. Functionality such as encryption should be built in. Audit trails must be able to show the patient everyone who accessed each part of their record. Decision support and health maintenance modules have become best practices in the electronic world.

Audits, breaches, and ROI changes should be top of mind for practices now, as they are on the increase and show no signs of slowing. HIM professionals will play a key role in dealing with all this change. If used correctly, HIM influence will result in improved outpatient outcomes, better business practices, and a safer healthcare environment for all.

Tips for Electronic Practices

- Perform due diligence on vendors
- Choose certified EHR software
- Ensure software is 5010 and ICD-10 compliant
- Visit existing clients and ask what works, what does not, and what functions they choose not to implement
- Put expectations into the contract
- Ensure audit software meets the needs of multiple audit types

Notes

1. Ponemon Institute. "2010 Annual Study: US Cost of a Data Breach." March 2011.
2. Department of Health and Human Services. "Annual Report to Congress on Breaches of Unsecured Protected Health Information for Calendar Years 2009 and 2010." September 1, 2011. www.hhs.gov/ocr/privacy/hitechrepts.html.
3. Department of Health and Human Services. "HIPAA Privacy Rule Accounting of Disclosures under the Health Information Technology for Economic and Clinical Health Act." *Federal Register* 76, no. 104 (May 31, 2011): 31426–49.

Lori Brocato is audit product manager, Steven Emery is director of product management, and Jan McDavid is general counsel and chief compliance officer at HealthPort.

Article citation:
Brocato, Lori; Emery, Steven; McDavid, Jan P. "Keeping Compliant: Managing Rising Risk in Physician Practices" *Journal of AHIMA* 82, no.11 (November 2011): 32-35.