COSMOS
Navigate the Compliance Universe

Compliance Today - December 2018
Compliance risk areas to consider for 2019

by Cornelia M. Dorfschmid, PhD, MSIS, PMP, CHC, and Catie Heindel, JD, CHC, CHPC, CHPS

Cornelia M. Dorfschmid (cdorfschmid@strategicm.com) is Executive Vice President & Managing Senior Consultant, and **Catie Heindel** (cheindel@strategicm.com) is Managing Senior Consultant at Strategic Management Services, LLC in Alexandria, VA.

As we entered into the last quarter of 2018, compliance officers and their committees likely began planning exercises for 2019, including developing Compliance work plans, drafting audit plans and review schedules, and identifying initiatives that are ripe for training and education. Both the Centers for Medicare & Medicaid Services (CMS) and the Department of Health and Human Services (HHS) Office of Inspector General (OIG) have emphasized the importance of conducting risk assessment and risk management activities to establish effective internal controls to remediate identified risks.

Risk areas

In today's highly regulated environment, there are always a multitude of compliance risk areas or issues emerging that may need attention or require planning. With that in mind, here are several major risk areas that will likely continue to be problematic for healthcare organizations and which compliance officers may wish to consider for 2019.

Arrangements systems

Contractual relationships with referral sources, also known as "arrangements," still remain high on the HHS OIG's radar and are a high-risk area that should be watched carefully. Any improper relationships between healthcare entities and providers, or others that potentially or actually violate the Stark Law or Anti-Kickback Statute (AKS), may be catastrophic. Improper relationships can taint hundreds or thousands of claims that could be deemed false. The fines per false claim have gone up (for violations occurring after November 2, 2015, the new minimum and maximum penalties are $10,781 to $21,563 plus treble damages). The loss and potential litigation can be very unsettling and extremely time consuming. This is magnified in the case of high-volume type claims (e.g., labs or diagnostic testing entities). To combat these risks, healthcare organizations should implement an internal system that outlines the process, policies, and/or procedures to monitor these arrangements, as well as a regular schedule for conducting reviews or validation audits of these types of transactions to ensure the systems and internal controls over contracting actually work. Arrangements systems should be designed to implement and document the four key procedural aspects of contracting: contract initiation, contract review, contract approval, and contract tracking.

Compliance officers must identify how contract oversight is implemented, particularly focusing on transactions or contracts that involve (directly or indirectly) the offer, payment, solicitation, or receipt of anything of value between the organization and any actual or potential source of healthcare business or referrals to or from the organization. Commonly, this is a risk area that pertains to contract management, which often is tied to vendor management. Although most larger health systems require vendors to register prior to making any payment transactions, smaller organizations may need to consider alternatives, including the use of checklists, contract

application forms, and stringent approval processes to get this area under control. Compliance should periodically audit arrangements and retain outside subject-matter experts if they do not have individuals with the right skill sets in-house.

Value-based payment programs (i.e., pay for performance)

CMS continues to align the quality of care delivered and the payments that providers receive through the strengthening of various CMS value-based payment programs. With numerous value-based programs now in operation, providers should ensure they are properly participating in the many relevant quality payment programs in order to maximize profit levels. As the healthcare industry has increasingly shifted toward models that consider quality-of-care metrics when reimbursing providers, it is essential for organizations to be able to ensure the accuracy of the quality data that they are compiling and submitting to the government or their payers.

Reimbursements under value-based payment programs work very differently from traditional fee-for-service models, because payment amounts are determined based on metrics reported to CMS — for example, specific measures developed to evidence the quality of the care provided or that evidence the overall health of a provider's population. Because providers are required to report on these quality metrics and demonstrate any clinical health improvements for their patients, it is essential that processes for measuring, calculating, monitoring, and reporting this data be implemented and tested to ensure accuracy and reliability. Oftentimes, this will involve working with a variety of vendors (e.g., electronic health record [EHR] companies, claims vendors, data analytic firms) to ensure that processes for gathering and verifying the data meet the requirements for each of the programs. It is essential that Compliance ensures these processes undergo comprehensive monitoring and auditing efforts to ensure that they are compliant, standardized, efficient, and effective.

Site-neutral payments

CMS continues to implement new payment policies in response to legislation that was passed as part the Bipartisan Budget Act of 2015 to address site-neutral payments.[1] Currently, Medicare payments for services performed in grandfathered, provider-based facilities (i.e., established on/before November 2, 2015) are more than 50% higher than payments for the same services performed in a freestanding facility, as long as certain requirements are met. In its recent round of proposed payment system rules for 2019, CMS is continuing to expand its focus on site-neutral payments between what Medicare pays for at traditional physicians' offices and at off-campus provider-based facilities (i.e., hospital clinics), where service rates are higher because of added hospital facility fees. Healthcare organizations operating provider-based facilities should continue to focus auditing and monitoring efforts to ensure that:

- their clinics meet all the provider-based requirements,[2]
- CMS attestations for provider-based status are obtained through local Medicare Administrative Contractors (MACs), and
- appropriate PN and/or PO billing modifiers and place-of-service (POS) codes (POS 19 or POS 22) are used when billing the services provided.

Compliance officers should also ensure that there is an organization-wide process in place for making Compliance aware of instances when new departments or clinics are established or existing clinics or departments are modified (i.e., they move to other buildings/locations) to ensure that the provider-based rules continue to be met and, where possible, the entities may maintain their "grandfathered" status.

Evaluation and management (E/M) services billing modifications

Billing for E/M services remains a high-risk area. E/M codes are among the most frequently billed codes by physicians and remain under scrutiny, especially codes indicating high-intensity level E/Ms in office and clinic settings (e.g., CPTs 99214/99215, 99204, 99205). Billing E/M codes with modifier 25 (indicating significant, separately identifiable E/M service by the same physician on the same day of the procedure or other service) also deserves vigilance. Compliance officers should be aware of the controls that are in place to handle these types of claims accurately.[3]

Another new development is the proposed changes that CMS has recently made to E/M billing. On July 12, 2018, CMS issued a proposed rule that includes a discussion of "Streamlining Evaluation and Management (E/M) Payment and Reducing Clinician Burden" under the Medicare Physician Fee Schedule for 2019.[4] To improve payment accuracy and simplify documentation, CMS is proposing to allow practitioners to choose to document E/M visits using medical decision-making or time instead of applying the current 1995 or 1997 E/M documentation guidelines; or, alternatively, practitioners will be able to continue using the current framework.

As a corollary to this proposal, CMS intends to apply a minimum documentation standard where Medicare would require information to support a level 2 CPT visit code for history, exam, and/or medical decision-making in cases where practitioners choose to use the current framework, or, as proposed, medical decision-making to document E/M level 2 through 5 visits. They also proposed new, single blended payment rates for new and established patients for office/outpatient E/M level 2 through 5 visits and a series of add-on codes to reflect resources involved in furnishing primary care and non-procedural specialty, generally recognized services.[5]

Different specialties may be impacted differently, depending on their typical E/M profiles, which are demonstrated via bell curves. If implemented, this rule will impact many monitoring programs, training programs, auditing protocols, and billing processes. Billing accuracy under this new rule needs to be pursued as a corporate strategy. Compliance officers and committees need to actively analyze and follow these developments.

Vendor monitoring and oversight

Employing vendors to carry out portions of business operations remains a high-risk area. CMS, within both its Medicare and Medicaid managed care regulations, outlines their expectation that entities have processes in place to identify, manage, and monitor their vendors, particularly those accessing HIPAA protected health information (PHI). Entities should be able to demonstrate a process to ensure that vendor contracts contain provisions to meet all applicable requirements related to the vendor activity, including those related to responsibilities as business associates under HIPAA and compliance-related requirements, such as training completion, sanction screening activities, conflict-of-interest certifications, and cooperation with internal/external review and audit activity.

Dashboards to evidence vendor performance should also be used to benchmark whether the vendor is performing its responsibilities in line with the contract provisions and whether additional monitoring is needed. Where issues with vendors are identified, organizations need to be able to show that investigations were conducted in a timely manner and, where corrective action was determined necessary, that this action was taken. Compliance officers need to monitor whether adequate documentation is maintained to reflect the organization's vendor monitoring and oversight efforts — complete documentation is best!

Cybersecurity of patient information

The constantly evolving privacy and cybersecurity landscape and the propensity for human error that results in

breaches require great vigilance. Organizations must be diligent in tracking and reporting potential or actual breaches, taking necessary corrective actions, and preparing at the individual and system level to guard against security incidents. This includes implementing procedures to regularly review records of information of system activity, such as audit logs, access reports, and security incident tracking reports. Monitoring procedures and systematic analysis of user and system activity can help detect ordinary and irregular action patterns. It is essential that healthcare entities learn from each other's mistakes and work with local law enforcement to detect security incidents that may impact the confidentiality of their patient information, as well as the reputation of their organization.

Additionally, many states, territories, and international bodies have recently enacted their own privacy and security laws that may impact healthcare operations here in the United States. For example, the General Data Protection Regulation (GDPR), now being enforced by the European Union (EU), has privacy implications for healthcare entities that treat or have treated patients who reside in the EU. It is essential that organizations maintain a system to track all relevant international, federal, state, and local laws and regulations related to privacy and security that may impact them, because provisions from these laws may not be consistent and may dictate that additional practices apply for specific patient situations.