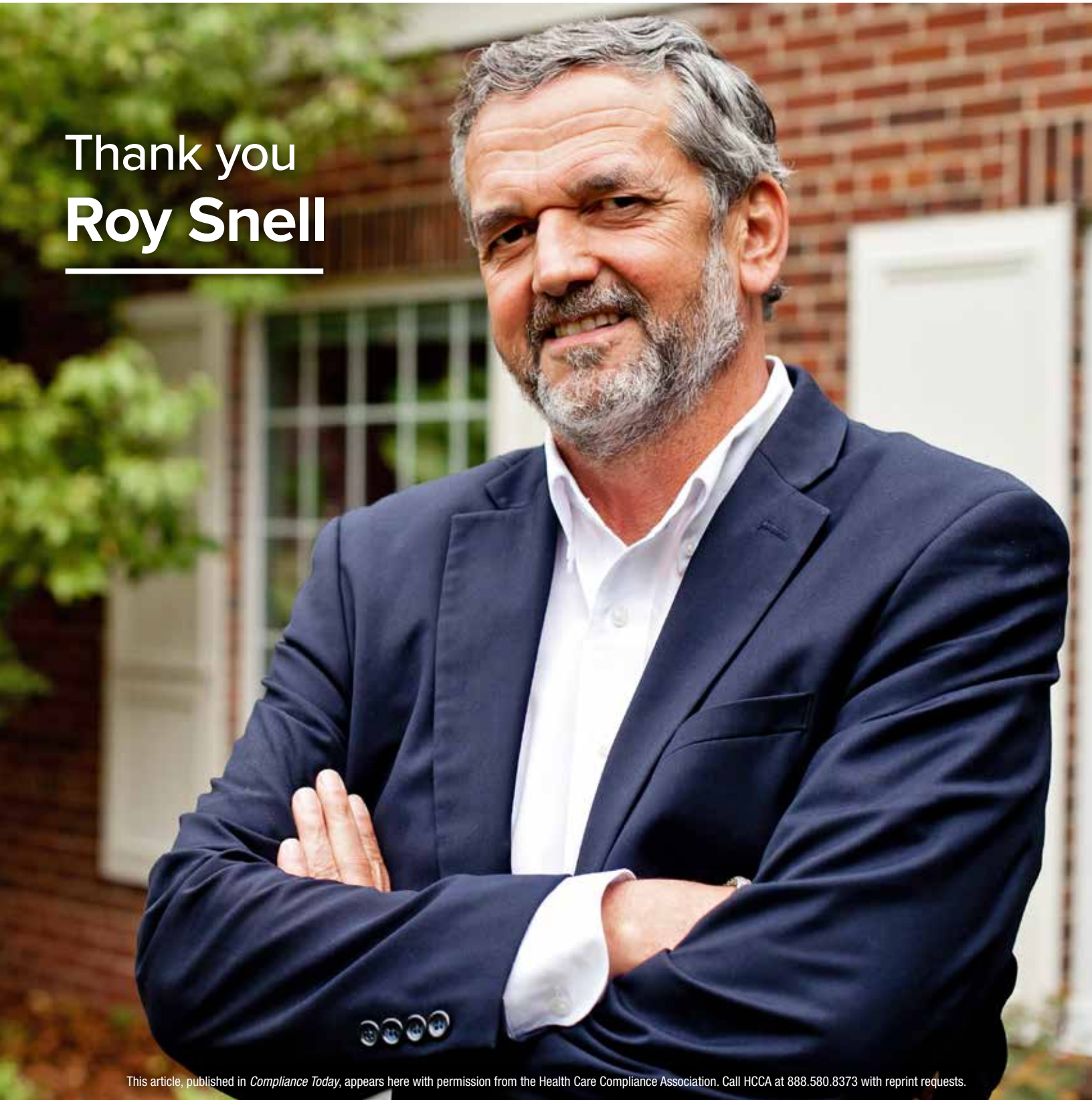
HCCA
hcca-info.org

Compliance TODAY

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

DECEMBER 2018



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

Compliance risk areas to consider for 2019

» Compliance officers should implement a centralized risk assessment and internal review process that identifies risk areas central to their operations for 2019.

» Healthcare-specific topics, such as arrangements with referral sources, value-based payment programs, site-neutral payment policies, billing for E/M services, and security of protected health information warrant proactive risk mitigation strategies.

» Organizations can use data analytic strategies and monitoring efforts for CMS contractor activity to determine risk areas that may emerge in the coming year.

» Financial error rates, hotline closure rates, training compliance rates, contracting compliance rates, and signage or notice compliance rates are a few metrics to consider for evidencing compliance program effectiveness.

» Delivering subject-matter expert training to the board to address emerging risk areas will help increase and improve their oversight abilities.

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.

Dorfschmid

Heindel

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.

It is essential that healthcare entities learn from each other's mistakes and work with local law enforcement to detect security incidents...

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.

CMS Targeted Probe and Educate audits

CMS Contractor audits continue. The new audits conducted by MACs, called Targeted Probe and Educate (TPE), are also ones to watch. Medicare providers need to be familiar with this new auditing strategy.[6,7] CMS's goal with this new medical review program is to reduce payment errors by identifying and addressing billing errors concerning coverage and coding made by providers. MACs are tasked with proactively identifying patterns of potential billing errors made by providers through data analysis activities and evaluation of other information, such as complaints, CERT data, Recovery Audit Contractor (RAC) vulnerabilities, and OIG and Government Accounting Office (GAO) reports. Once a pattern is identified, MACs must take action to prevent and/or address the identified error and publish local medical review policy (i.e., Local Coverage Determinations) to provide guidance to the public and medical community about when items and services will be eligible for payment under Medicare. CMS also publishes Medicare Learning Network educational articles as they relate to the medical review process.

Although there is some focus on education, given that MACs have the opportunity to give providers detailed one-on-one feedback, it must also be understood that very often aggressive corrective action and corrective measures will be taken, beyond just sample analysis and payback. MACs use data analysis to identify providers and suppliers who have high claim-error rates or unusual billing practices, bill items and services that have high national error rates, and are a financial risk to Medicare. Providers whose claims are compliant with Medicare policy won't be chosen for TPE.

The majority of providers that have undergone the TPE process have increased the accuracy of their claims. However, any problems that fail to improve after three rounds of education sessions will be referred to CMS for next steps. These may include 100% prepay review, extrapolation, referral to a RAC, or other action—all of which should be avoided. The most common problems reported by CMS involve physician signatures, medical necessity documentation, eligibility, and missing or incomplete certifications/re-certifications. TPE reviews deserve attention by both providers and compliance officers. Organizations should consider designing metrics to monitor compliance with potentially problematic areas (e.g., physician signature compliance rates) that may be focus areas for local MACs.

But remember, if the government can examine a provider's data, so can the provider.

Data analytics

Government contractors, such as MACs, RACs, and Unified Program Integrity Contractors (UPICs), and the HHS OIG are increasingly relying upon data analysis and data analytics to detect patterns and potential violation of Medicare and payer rules and regulations in claims. But remember, if the government can examine a provider's data, so can the provider. Providers need to become more proactive and invest in examining their own claims data on a routine basis.

Basic data analysis can go a long way. It does not have to begin right away with

complex modeling, pattern analysis, predictive analytics, or regression. For example, compliance officers may want to receive reimbursement analysis on E/M profiling by specialty from their Revenue Cycle management function and determine if and how they monitor unusual profiles and deviations. A simple analysis of billing for deceased patients, checking for duplicate billing (e.g., same day, same patient service/item), analyzing very long length-of-stay claims, or highest dollar claims (top 1%) is helpful.

When it comes to contracting and physician arrangements, tabulating if the written contract has the required business associate agreement, fair market value documentation, and appropriate signatures may be a simple analysis that may uncover some important compliance gaps. Together with the compliance committee, the compliance officer may wish to pursue a data quality strategy, including monitoring and oversight of the quality of data gathered and used. Compliance officers may also find that receiving and analyzing periodic monitoring reports on timely resolution of credit balances is beneficial.

Centralized risk assessment and internal review

To pass muster with OIG and government expectations, it is not sufficient to have a compliance program; it must also be effective. One way to get there is by implementing a "Centralized Risk Assessment and Internal Review" process, which has become a specific requirement in many of the more recent corporate integrity agreements (CIAs), which can serve as a best practice or helpful guide. The purpose of the risk assessment exercise is to identify and address risks associated with a provider's activity in the federal healthcare programs, including but not limited to the risks associated with the submission of claims for items and services furnished to Medicare/Medicaid program beneficiaries, arrangements and contracting with providers, patient safety, etc.

The risk assessment and internal review process typically requires Compliance, Legal, and other department leaders, at least annually, to:

- Identify and prioritize risks,
- Develop internal audit work plans related to the identified risk areas,
- Implement internal audit work plans,
- Develop corrective action plans in response to the results of any internal audits performed, and
- Track the implementation of the corrective action plans in order to assess the effectiveness of such plans.

Providers may have implemented risk assessment processes in some shape or form, but these often lack the formality (e.g., probability/impact scoring), continuity, or approved methodology expected by the OIG, because they rely on stove-piped approaches rather than a truly "centralized" approach. Compliance officers must be able to receive reports on their internal monitoring and receive information that includes metrics or measures to be able to assess performance improvements and improving trends. Revisiting this area in 2019, evaluating the sophistication and comprehensiveness of reports, and strengthening these processes would be wise and a good investment in any compliance program. It will also facilitate providing the needed assurances for board oversight.

Compliance metrics

Compliance program tools and methods have become more sophisticated over the years. However, given the increased availability of data on almost anything, even compliance programs have become more measureable. In

March of 2017, OIG issued guidance with the *Measuring Compliance Program Effectiveness: A Resource Guide.*[8] One growing trend in the enforcement community is an interest in metrics and measures when effectiveness needs to be demonstrated. The more indicators and metrics are measured, the better violations can be prevented and the fewer headaches with corrective actions.

In billing compliance, both coding accuracy rates and financial error rates (e.g., percentage of paid reimbursement amount in error) are metrics to help with monitoring and assessing if issues are severe, systemic, or only sporadic mistakes. Many CIAs still use the 5% threshold rate for the financial error rate (FER) as a guideline triggering extrapolation, although OIG has done away with it in recent CIAs. Now, the burden of the decision of when to go from sample to extrapolated claims overpayments is left to the providers. Aside from the FER, hotline issue closure rates, training compliance rates for mandatory general and specialized compliance training, contracting compliance rates in arrangements reviews, and signature or notice compliance rates (e.g., Notice of Privacy Practices, Medicare Outpatient Observation Notice, Important Message from Medicare Notice) are just a few other metrics to consider. Adding at least one new metric should be a goal for the Compliance Office.

Board education to enable oversight

The OIG, in its various compliance guidance documents, has consistently emphasized the importance for boards of directors to understand and be fully engaged in their oversight responsibility. A critical element of effective oversight is the process of asking the right questions of management to determine the adequacy and effectiveness of the organization's compliance program, as well as the performance of those who develop and execute that program. However, oftentimes board members may not have the subject-matter expertise necessary to properly understand and question operations related to high-risk areas. As such, it is essential that board members are educated on the legal and compliance risk areas they may face, including potential implications arising from non-compliance, so they are able to question proposed management decisions impacting these areas.

Conclusion

In light of the fact that most healthcare providers are dependent upon federal or state healthcare programs to provide payment for the services furnished to program beneficiaries, compliance with federal and state requirements is essential. With new legal and regulatory risk areas emerging every year, it is imperative that compliance officers remain diligent in monitoring the risks that impact their lines of business to ensure that their compliance programs are effectively managing and mitigating these risks.

1. See Section 603 of the Bipartisan Budget Act of 2015.
2. See 42 CFR 413.65 (Requirements for a determination… provider-based status)
3. Novitas Solutions: Modifer 25 Tips. Available at https://bit.ly/2J6LWkD
4. 83 Fed. Reg. 147, 37046, CMS: "Medicare Program: Proposed Changes to Hospital Outpatient Prospective Payment and Ambulatory Surgical Center Payment Systems and Quality Reporting Programs; Requests for Information on Promoting Interoperability and Electronic Health Care Information, Price Transparency, and Leveraging Authority for the Competitive Acquisition Program for Part B Drugs and Biologicals for a Potential CMS Innovation Center Model" July 31, 2018. Available at https://bit.ly/2NEUFzR
5. See CMS Fact Sheet "Proposed Policy, Payment, and Quality Provisions Changes to the Medicare Physician Fee Schedule for Calendar Year 2019" July 12, 2018. Available at https://go.cms.gov/2P5tzih
6. CMS: Targeted Probe and Educate (TPE): "When Medicare Claims are submitted correctly, everyone benefits." Available at https://go.cms.gov/2z6gArq
7. CMS: Targeted Probe and Educate: Flow chart. Available at https://go.cms.gov/2vfoKc1
8. See HCCA-OIG: Measuring Compliance Program Effectiveness: A Resource Guide, March 2017. Available at https://bit.ly/2MtT1MM