HCCA®
HEALTH CARE
COMPLIANCE
ASSOCIATION

Compliance TODAY

June 2014

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

An outside counsel with an inside track on healthcare compliance

an interview with Daniel Gospin

Partner, Health Care and Life Sciences Practice, Epstein Becker Green, Houston

See page 18

29
Expanding protection for whistleblowers
Shachi Mankodi and Hannah Levinson

33
Billing monitoring: Weakest link or greatest strength?
Cornelia M. Dorfschmid

43
The Physician Payment Sunshine Act: What physicians are asking
Jillian A. Watts

47
An interdisciplinary approach to compliance investigations
Laura M. Alfredo

by Cornelia M. Dorfschmid, PhD

Billing monitoring: Weakest link or greatest strength?

- Advances in technology and in health IT business operations mandate advances in compliance monitoring.
- Compliance must be made measurable to be managed well.
- Billing monitoring must be a match to data-driven and sophisticated enforcement efforts.
- Billing monitoring should develop and rely on metrics and benchmarks, formal methods, standardization, phasing, and sampling to make compliance more measurable.
- Billing monitoring should incorporate the financial error rate (i.e., net-overpayment error rate) as a metric.

Cornelia M. Dorfschmid *(cdorfschmid@strategicm.com) is Executive Vice President at Strategic Management Services, LLC, in Alexandria, VA.*

Compliance auditing and monitoring

It is well known from the various compliance program guidance documents issued by the Department of Health and Human Services Office of Inspector General (OIG) that any effective compliance program must contain an internal auditing and monitoring element. Auditing and monitoring should address both the compliance program with its own operations as well as the compliance high-risk areas that impact operational areas. Auditing and monitoring are crucial elements in establishing and maintaining an effective compliance program as well as a functioning system of internal controls.

Dorfschmid

Auditing and monitoring are also part of risk management activities designed to protect the healthcare organization, its workforce, customers, and assets from risk or harm.

Key characteristics that distinguish auditing and monitoring are independence, objectivity, and frequency. Competency and integrity, on the other hand, are common requirements for both. Often auditing and monitoring are also distinguished by focus. Auditing conducts testing of items or the output of a process, typically in a retrospective fashion (e.g., a list of claims, a set of contracts or arrangements, applications for health plan membership). Monitoring focuses on the business processes and determination of root causes of failures or system weaknesses. Monitoring looks at control settings and thresholds that can indicate when a process is out of control or not within bounds set by defined thresholds, metrics, or targets. Written policies and procedures, standard operating procedures (SOPs), workflow, technical software system settings and configurations, and any rules that trigger exceptions, work queues, or process holds for inspection are typical facets of a monitoring process.

In the context of monitoring risk, and especially billing risk, it is worth noting that the compliance officer does not hold the sole responsibility for addressing compliance risks. Rather, the compliance officer relies to a large degree on the internal monitoring of operational units with their particular skill sets and interacts with departmental quality assurance (QA) functions or internal monitoring functions as part of compliance oversight. The compliance officer conducts audits to verify that controls and monitoring are working or if internal monitoring is inadequate. Controls and monitoring should be part of any investigations or other high priority risk the compliance officer wants to address. Fundamentally, however, "Monitoring is primarily the responsibility of program managers and operational departments. The compliance officer should verify that monitoring by management is taking place and ensure that ongoing auditing verifies and validates this process."[1]

Then versus now—the game has changed

It is no secret that some of the biggest risks and one of highest compliance priorities in a healthcare organization arise from threats to its revenue integrity and, in particular, vulnerabilities in its billing and coding processes. Lapses in revenue integrity harbor the potential risk that inappropriate payments will be received from federal and state healthcare programs. Compliance officers therefore need to worry not only about risks that are actually identified, but also those that should have and could have been identified. They need to worry about what constitutes an effective billing auditing and monitoring program that operates in a reasonable, diligent, and effective manner. They need answers to the questions when and why their "proactive" efforts are sufficient and effective.

One would expect that after 16 years since the OIG's first compliance program guidance was released in 1998, the puzzle of how to conduct effective compliance auditing and monitoring, and especially billing auditing and monitoring, would be solved. Instead this remains an open question that is discussed more than ever. The simple truth is that compliance programs got a lot more complicated since then. Integrating compliance into business operations got more complicated. Business operations became more sophisticated and data-driven, due to the changes in health IT and the massive use and availability of health data, including electronic protected health information (ePHI) such as claims, payments, and electronic medical records. Furthermore, the Centers for Medicare & Medicaid Services (CMS) contractor reform brought us MACs, RACs, ZPICs, and MICs. They come with their sophisticated statistical tools and methods, and are paired with a stronger coordination of enforcement efforts: the Health Care Fraud Prevention and Enforcement Action Team (HEAT). These enforcement agencies and CMS contractors now have access to a vast number of claims and enrollment data, which they analyze and mine for inappropriate payments and suspicious billing patterns. They also extrapolate overpayments from relatively small samples and identify suspicious billing patterns through data mining that organizations may have no inkling of. What to do?

> One would expect that after 16 years… the puzzle of how to conduct effective compliance auditing and monitoring… would be solved. Instead this remains an open question that is discussed more than ever.

If healthcare organizations want to thrive and survive in this data-driven and sophisticated enforcement era, their proactive monitoring efforts need to be a full-fledged match to CMS, HHS OIG, and government contractors' data analysis and enforcement efforts. Therefore they must make compliance *measurable* to manage risk. The game has changed and a billing monitoring program can be the greatest strength in a healthcare organization's war chest, if it leverages the organization's own information, data, and people. But, it can also be the weakest link if not done, not done right, or not done aggressively enough. Compliance officers need to seek assurance that billing monitoring provides hard evidence that paid claims are processed correctly, or otherwise uncovers gaps. They need to get answers to "How do we know it works?"

Billing monitoring—critical success factors

Old solutions for billing monitoring won't meet today's challenges. A weak billing monitoring program operates under few, weak, or ill-defined controls without sufficient leadership and routine. A strong billing monitoring program sets reasonable controls and updates, and tests those controls routinely. Internal monitoring through those units involved in preparing and contributing to claims, namely health information management (HIM), case management, patient financial services, or the business office, need to be called upon and be required to show evidence of quality assurance (QA) efforts and/or functions. Compliance, in turn, should take leadership and call upon these QA functions to report on the quality of their processes and provide factual evidence why they work (i.e., performance, compliance, or accuracy metrics). Compliance can assist and advise on measures and metrics being used and developed for that purpose, but can also conduct oversight of the adequacy of such measures and metrics. In other words, the compliance officer should worry about too lax controls being applied in the business units and set forth by QA units to get to a "pass" versus a "fail." In addition, vague measures that are inconclusive and won't hold anyone accountable must be checked for.

Factors for success

The following factors describe successful billing monitoring programs and may be considered when implementing or strengthening a billing monitoring program.

Leadership

Compliance should take leadership and exercise oversight of QA functions in the business units, in particular the billing office, case management, HIM, and patient access. Compliance has to rely on these units and their expertise for internal monitoring. The monitoring efforts are not independent (like audits), but because they are done internally by the various departments, they need some external oversight and guidelines. Compliance should set expectations for what these QA units need to report to provide assurances that they are self-policing adequately, such as hard numbers and statistics or metrics that evidence that pre- and post-pay billing are functioning properly. Compliance needs to lead them along this path and support them in developing some of the metrics.

Replicability and routine vs. non-routine

The assurance efforts of billing monitoring programs need to be repeatable so that tracking and trending is possible. They should rely on both routine and non-routine approaches and written procedures that define clearly when monitoring progresses from routine to non-routine or focused efforts. For example, a procedure might call for escalation whenever a physician's consecutive error rate rises above 30% in test samples over a three month period in a monthly physician billing monitoring program. Such failure rates may then trigger focused monitoring with 100% concurrent review of the physician's claims along with other corrective action, such as training or deeper dive audits. Well-defined triggers from routine to non-routine monitoring are critical.

Standardization

Using a standardized process to monitor how billing is monitored across facilities or business units facilitates replicability, trending, and aggregation. Any results of QA efforts should be reported up the chain of command. Planning ahead what a useful QA report to Compliance on quality assurance efforts might look like will be helpful to HIM, billing and reimbursement, case management, or others. Developing and providing report templates will facilitate the reporting process and analysis. Reports should include not just absolute numbers and data (such as volume), but metrics or measures on claims or process data (e.g., accuracy, error, compliance, or completion rates or scores) as well. Standardized review templates and analyses allow for developing and comparing such rates and aggregation, or comparison across business units or time periods.

Communication and reporting

One of the key features of a successful billing monitoring program is frequent communication between Compliance and the QA units in business operations. Periodic reporting of evidence of QA's internal monitoring efforts to the compliance committee, supported with evidence in the data, should be mandated. Performance measures and claims error or accuracy rates should also be periodically reported to the board, along with any needed steps for corrective action planning (CAP). Logs of CAP steps should be developed, and billing monitoring ensures that controls are amended based on CAPs. Without adequate reports of monitoring results and follow-up action, there is no accountability and transparency as to the scope and level of assurance actually provided. The danger of ambiguous or vague reports without metrics and measures is that it will leave everyone wondering "Why didn't we know about these claims?" when incidents or enforcement action happens and recovery demands or false claims allegations are made.

Formality and method

Targeting certain risk areas or operational units for monitoring should have a good reason. It is best founded on a risk management approach that is sufficiently formal and comprehensive. Risk identification and assessment are best conducted with proven methods, such as using probability-impact analysis and risk scoring. The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) enterprise risk assessment method may provide additional input for developing an approach.[2] For purposes of billing risk and risks to revenue integrity, a risk list or risk universe should be developed collaboratively with the operational units and support from the compliance committee. Methods of measuring the risk should be discussed with the compliance committee to create buy-in so that outcomes of risk scoring are credible and actionable, and hence can provide input for monitoring. Criteria should be developed for assessing which billing risks would be acceptable, which would warrant immediate remediation and further auditing or monitoring, and which may have further review postponed. Ultimately, a formal method provides numerical results that make scorings and ratings transparent and provides an opportunity to agree or disagree. Boards will appreciate the clarity.

Metrics

Metrics are rates or benchmarks that either should be achieved (e.g., coding accuracy rate) or not be exceeded (e.g., financial error rate) and keep processes controlled. Benchmarks are part of an effective billing monitoring program. They set triggers and flag a potential problem that warrants follow up with an audit or root cause analysis. For example:

- **Net-overpayment error rate** (financial error rate) in statistical samples, such as discovery samples of 50 claims. Note that HHS OIG allows a 5% financial error rate in claims reviews conducted by Independent Review Organizations in corporate integrity agreements (CIAs). This threshold rate of 5% in CIAs, when exceeded in a discovery sample, typically triggers an expanded claims review as well as root cause analysis of the claims process. The financial error rate as a metric should be integrated into billing monitoring using paid claims samples. Although 5% is a rate set for organizations under CIAs, it is not a general requirement, but it can serve as a goal. The Compliance department and compliance committee should work together on setting the appropriate level that triggers follow up action.
- **Coding accuracy rate** is a metric that should be used and reported on, including trends. For example, a best practice standard recommend by AHIMA is 95%.[3]
- **Training completion rates** for compliance and professional billing or coding staff can be considered.
- **Claims denial rates** should be examined and tracked.
- **Physician evaluation/management (E/M) level profiles** can be developed and tabulated monthly or quarterly. A metric that flags any physician with more than a certain deviation from the average level for a specialty can be developed. The average can be a national norm or entity-internal benchmark, such as average E/M level for new patients billed by all internists or all cardiologists of the healthcare organization or practice, etc.
- **Electronic medical records** (EMR) are subject to compliance risk due to inappropriate copying and pasting. Metrics developed from the audit logs of the electronic health records (EHRs) can be developed and allow for flagging potential problems when providers have combinations of high volume of records or lengthy records paired with very short online usage time. It is noteworthy that the OIG put emphasis on audit logs and the uniqueness of EHRs as useful tools in validating medical records.[4]
- **Error rates for probe samples of claims** that fall into outlier ranges in PEPPER reports can be developed.
- **Patient Status change rates** pre- and post- the "two midnight rule" by CMS that changed requirements for observation and admission. On average, patient care should not change, so any significant changes in how patient status is assigned may be a flag.

> Expansion to large samples and deeper dives based on input from small sample monitoring results should follow a procedure, rather than be ad hoc decisions.

Escalation and phasing

Billing monitoring is best conducted with defined escalation procedures and phased approaches. Starting small is fine for routine monitoring. Expansion to large samples and deeper dives based on input from small sample monitoring results should follow a procedure, rather than be ad hoc decisions. For example, if billing monitoring uses sampling, a standardized process might include a progression from a Phase 1 with small set of samples (such as 3-10 judgmentally sampled prepaid or post-paid claims per month and provider), to a Phase 2 with 30 claims in a Probe sample, and then to a Phase 3 with 50 claims in a statistical Discovery sample, for any provider who does not meet set benchmarks for each phase. Furthermore, the financial error rate in a Discovery sample of 50 paid claims could be used along with a requirement that triggers reporting to Compliance (e.g., whenever a financial error rate exceeds 40%). Only if necessary and based on defined decision process are Full samples then conducted next as Phase 4. Note that OIG recently updated the Self Disclosure Protocol for Providers[5] and now requires at least 100 claims in Full samples. That may be a guide as to the minimum size whenever overpayment extrapolation from claims samples becomes necessary. A written policy and procedure or defined decision process that contains a threshold of when to go the next level and describes the phasing is advised.

Sampling and data mining

To meet today's challenges and address the many billing risk areas, it will be necessary to use sampling effectively and efficiently to conserve resources. Both judgmental and statistical samples can be used. It is, however, important to note that any objective projection from samples to a universe of claims or items is only possible with statistical samples. Statistical samples typically require a randomizer software. Haphazardly pulling charts from a pile or a list would not qualify as statistically random. Regarding sample sizes, it is helpful to go from small to large progressively as one investigates a problem.

Lastly, a billing monitoring program should include at least some efforts toward data analysis and data mining with more sophisticated methods of detecting patterns in paid or prepaid claims data. For example, queries to flag billing for dead people, mining for providers on sanction lists, and weeding out duplicate claims (e.g., same date of service, same beneficiary, same service) are just touching the basics of these approaches. If Compliance finds that nobody within the organization is looking at data that way, they should organize a group or task force to assess the feasibility of claims data analytics within the organization. This is typically a joint effort between Compliance, the IT Department, Patient Financial Services, or Revenue Cycle and HIM. Statistical expertise can be added as necessary. System edits such as the National Correct Coding Initiative (NCCI) and medically unlikely edits (MUE) are a minimum, but they are far from all that is necessary to be a valid match to recovery and fraud audit contractors' activities in data analysis and data mining.

Conclusion

It behooves compliance officers to reassess what is done in billing monitoring for the organization and whether it can pass muster in today's era. Pronouncements that billing and coding processes work well should be supported by factual evidence, including metrics that support such facts and describe how systems are controlled. If anything, the financial error rate should be included in the war chest of those implementing and overseeing billing monitoring. It can contribute to making a billing monitoring program one of the entity's greatest strengths rather than its weakest link.

[1] C. Dorfschmid, S. Forman: "Meeting the Challenge of Adequately Addressing Numerous Compliance Risks." *Journal of Health Care Compliance,* September/October 2013, p. 21.
[2] See www.coso.org
[3] See American Health Information Management Association (AHIMA) Distance Education: "Benchmarking Coding Quality." July 24, 2008. Audio seminar/Webinar. Available at http://bit.ly/1mDioZ8
[4] Department of Health and Human Services OIG: CMS and Its Contractors Have Adopted Few Program Integrity Practices to Address Vulnerabilities in EHRs. January 2014. OEI-01-11-00571. Available at http://1.usa.gov/1fVwo24
[5] Department of Health and Human Services OIG: Updated OIG's Provider Self Disclosure Protocol. April 2013. Available at http://1.usa.gov/18NDCw9