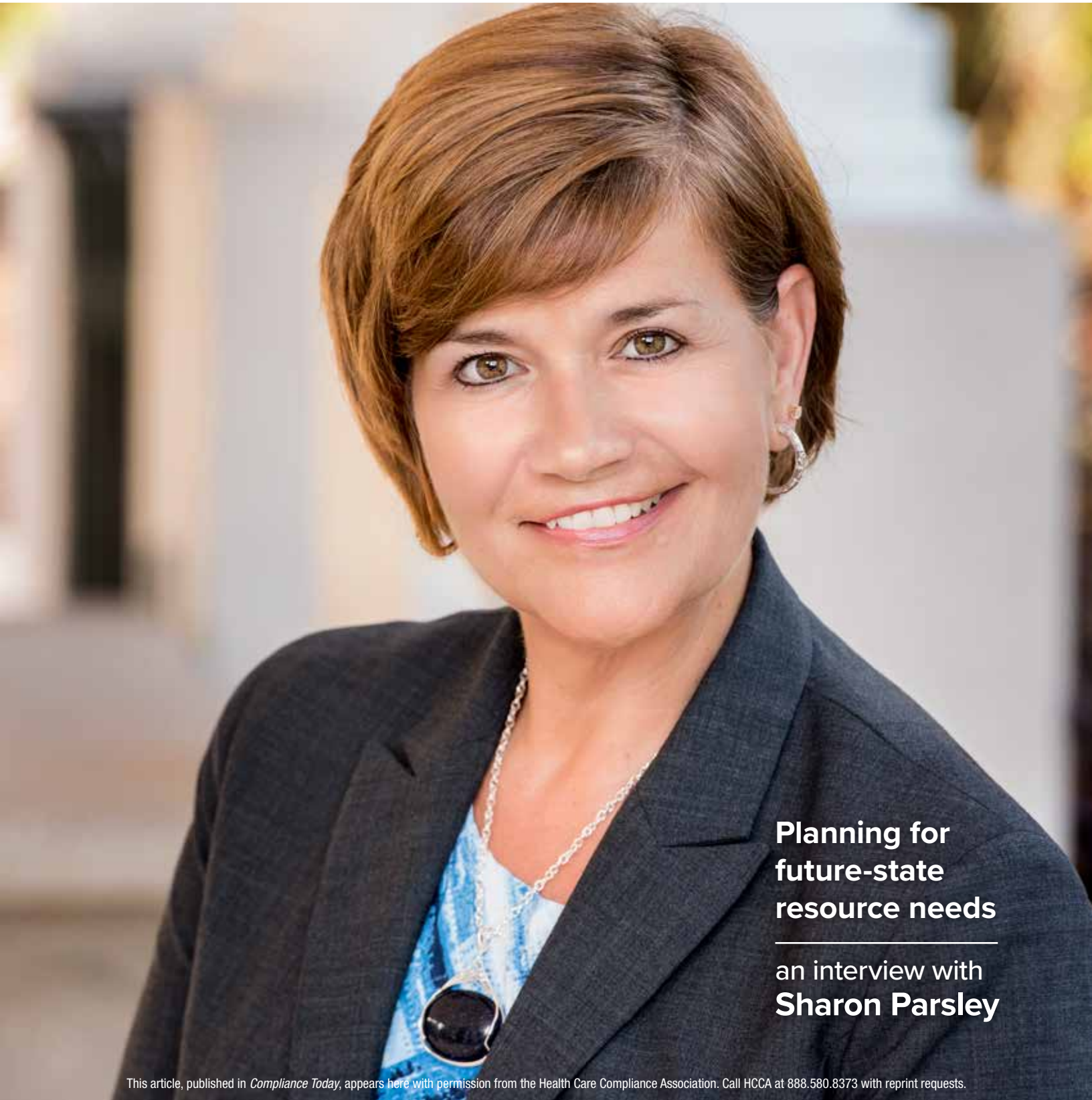
HCCA
hcca-info.org

Compliance TODAY

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

OCTOBER 2018



Planning for future-state resource needs

an interview with **Sharon Parsley**

by Marti Arvin

Effective auditing and monitoring for your compliance program

» The terms *auditing* and *monitoring* have different meanings.
» Not all monitoring needs to be done by the Compliance Office.
» Leverage other departments to expand the compliance auditing and monitoring program.
» The governing body, not Compliance, is responsible for risk tolerance decisions.
» Compliance work plans are not set in stone; they can be adjusted.

Marti Arvin *(marti.arvin@cynergistek.com) is Vice President of Audit Strategy at CynergisTek, in Austin, TX.* /bit.ly/in-MartiArvin

What is effective auditing and monitoring in support of an effective compliance program? There is no clear-cut answer, but it is clear that doing nothing will not get you to effectiveness. The key question is how much of something must be done? It is helpful to understand what the two terms mean. They are often used as a single phrase, but the two activities are distinctly different. Understanding what the two activities entail can help determine if what is being done supports an effective compliance program.

Arvin

Auditing versus monitoring

An audit is usually a formal, structured process with a defined scope of work to evaluate controls and determine if a process is functioning as expected. An independent, objective, and knowledgeable third party should perform it. The scope of work would generally define what controls are being tested, the universe from which a sample is being identified, the method for randomly selecting the sample, and the size of the sample that will be evaluated. It might also include a background regarding why the audit is being performed and the identified references and resources used in support of the audit.

Some organizations refer to activity under this element of the compliance program as "reviews" rather than audits, because they recognize what they are engaged in does not have the structure and formality of a true audit. The important factor is to understand the difference in the terms and use them appropriately.

Monitoring does not have the same requirement for independence and objectivity that auditing does. Monitoring is something that can be performed by the Compliance Office as an independent party, but it can also be a self-assessment performed by the business operations unit. Monitoring is often conducted on a more routine, less formal basis

than performing a review or an audit. For example, there may be a requirement that all clinical areas complete a self-assessment of coding and documentation practices by selecting ten claims a month and evaluating the accuracy and completeness of the coding and documentation for those services. Because the business unit that performs the work conducts the monitoring, it cannot be considered an independent and objective assessment. That is not to say that the person performing the monitoring will not do a thorough and complete job—it is simply a recognition of the inherent conflict of interest in having someone involved in the process also evaluate the process.

Now that the terms are defined, what are the next steps? The key to effective auditing and monitoring will encompass a number of factors. Key among those are:

- Conducting an effective risk assessment and risk prioritization for the organization,
- Identifying resources to conduct auditing and monitoring activities around the high-risk items, and
- Actually performing the auditing and monitoring activities.

The risk assessment process and risk prioritization

The buy-in of senior leadership and business unit leaders is critical to conducting an effective risk assessment. The compliance officer will be able to identify a number of risks the organization has and provide input into the priority of those risks, but the ultimate decision regarding the risk tolerance of the organization lives with the senior leadership and governing body. There may be risks the compliance officer is not aware of, and even for the risks known by the compliance officer, there may be compensating controls that would impact the overall priority of addressing such risks.

Compliance may drive the risk assessment process, but the final outcome—a prioritized list of the organization's risks based on the likelihood of the risk occurring, the consequences if it occurs, and mitigating factors (e.g., compensating controls)—must be determined by the governing body. This final list will be the road map to the auditing and monitoring program. Rarely does a compliance program have the resources to address all risks but, ideally, the organization will provide sufficient resources to address the highest risk. The decision on which risk will be addressed through the auditing and monitoring program should be formalized in the minutes of the oversight body for the compliance program. It should be clear that the governing body was made aware of the risks, made the final decision regarding which risks would be addressed, and how they determined which resources they would use to address them. If the risk assessment identifies ten high-risk items, but the resources are not available to address all ten, it is important that the governing body is clear on the potential consequences of not addressing each risk or providing support to obtain the resources.

A mistake made by some compliance professionals is to attempt to address all the high priority risk items with the resources available, if their governing body is not willing to support additional resources. This approach can have multiple negative consequences. It can lead to staff burnout because of overwork, sloppy work because of the pressure to complete more audits and reviews than feasible, and/or a continued unwillingness for the governing body to provide resources if they perceive the risks are being addressed.

Compliance professionals should be very clear to the governing body that if they choose not to provide sufficient resources to address the highest priority risks, those risks will not be part of the annual auditing and monitoring

work plan. Decisions on risk tolerance should be left to the governing body. The compliance professional may have to fight the inherent natural desire to assure all the high-risk items are addressed in the interest of protecting the organization.

The risk assessment process may be a joint effort with other business units, such as Risk and/or Internal Audit. Not only does this get Compliance the input of these business units, but it also means Compliance will not be standing alone in presenting the risks to the governing body. It also allows for the coordination of efforts that may result in a more efficient use of resources to address more risk areas.

When identifying risk, most organizations will take into account a number of resources. The Office of Inspector General (OIG) Annual Work Plan[1] is one such often-used resource—but it should not be the only resource. Looking at other program integrity and enforcement activities of any regulatory body that has oversight for activities performed by the organization will be important. There can be a multitude of these in addition to the OIG. Those of interest to the organization will depend on the nature of the organization and the laws and regulations it is subject to, but they may include the Office for Civil Rights (OCR), the Food and Drug Administration (FDA), the Office for Human Research Protections (OHRP), and the Department of Justice (DOJ), just to name a few.

Resourcing the auditing and monitoring function

There is nothing that says all auditing must be done by the Compliance Office. By coordinating with Internal Audit, the Compliance Office may be able to leverage Internal Audit's expertise and resources to cover some of the high-risk areas. This alleviates the need for resources in the Compliance Office to conduct additional audits, reviews, and/or monitoring. Leveraging other resources is particularly important for small healthcare entities.

The key here is to identify what audits need to be conducted, based on the risk assessment and risk prioritization, and then match the available resources. The matching of available resources also means looking at the available expertise. Compliance may have expertise that Internal Audit does not and vice versa. Being thoughtful in this regard allows for the maximum utilization of resources as well as helping to avoid duplication of effort. Business units get frustrated if multiple parties appear to be looking at the same thing, and coordinating helps make this process smoother. Ideally, Compliance would not want to conduct an audit of the same business unit at the same time as Internal Audit conducts a separate audit of that same business unit.

The key here is to identify what audits need to be conducted and then match the available resources.

Matching expertise may also mean recognizing the required expertise might not exist in the organization. If there is a need to perform an audit of Information Security processes and controls, or an assessment to assure the appropriate processes are being followed for clinical trial billing, there may not be a resource in Compliance or Internal Audit with the necessary skill set. Therefore, this type of audit may need to be outsourced to a third party and would likely require budget approval. Being very clear about the expertise and skills available internally and the risk to

be addressed are critical to assuring senior leadership understands the consequences of not providing support or the appropriate resources.

The Compliance Office does not need to handle all monitoring activities. If Compliance can partner with business units and others, there can be ways to leverage other talent and resources available. For example, if the Compliance Office has oversight for privacy, a checklist could be created for each of the clinical areas to complete on a routine basis for a defined number of activities. This may entail having a clinic or nursing unit manager conduct a walk-through to evaluate compliance with the various items on the checklist. There can be flexibility for how one department does this over another. If the criterion is to complete the checklist once a month, one manager may do the entire checklist on one specific day, while another may spread it out over the month. Either way, the goal is to help ensure the walk-through assessment is completed once a month. The compliance officer could then collect the assessments and identify any issues for a particular business unit or a trend across business units.

The same walk-throughs can be done by the compliance officer instead, but that depends on what resources are available. In addition, a third option is to include this type of monitoring as a component of other activities. Using the same privacy monitoring example, if there are process improvement activities occurring and there is a regular check of the clinical areas by the individuals involved in that effort, they might be able to evaluate the checklist items during the course of their assessments for process improvement. Just like the overall process, it requires buy-in of senior leadership.

If the plan is to have business units perform monitoring activities, but they get the sense this is not important to senior leadership, they may be less likely to participate. If this is how the organization elects to address risk, then the business owners need their leaders to deliver the message that it is an expectation for them to cooperate and complete monitoring activities in the form and format prescribed.

Another way to help ensure accountability is to report metrics to senior leadership on a routine basis. This allows the business unit managers to know how effectively they are meeting the expected monitoring activities. Tying this metric to performance appraisals and incentive plans is also an effective way of getting participation.

An important factor for the Compliance Office to keep in mind is that monitoring will likely be perceived as an additional step above and beyond what the manager views as their responsibility. Creating a monitoring function that is effective but not unduly burdensome will help adoption. Going back to the example of the privacy checklist discussed earlier, there may be 50 items that Compliance would ideally like to have monitored, but paring that list down to 10–20 would make it less burdensome on the business manager. There may be some that are considered more critical, but consideration must also be given to those that would be quick and easy to incorporate into functions already being done. For example, a list of 20 items, 10 of which can be completed quickly, may be more effective than a list of 10 items if all 10 require more overall effort to complete. Allowing flexibility in the method of completion also allows the manager to best match the ability to complete the checklist with their workflow.

Effectively resourcing the audit and monitoring activities requires a clear understanding of the risks and risk prioritization, the available resources within the organization, the willingness of senior leadership to hold business units accountable for the activities, and

clear documentation of how determinations were made regarding which risks the organization would focus on. The documentation should include not only a clear annual auditing and monitoring work plan, but should also include meeting minutes of the discussion and approval of the work plan by the governing body with an explanation, if applicable, of why certain high-risk items were not included in the work plan.

Conducting auditing and monitoring

The actual fun begins once a work plan is approved. All audits performed under the work plan should have a formal scope of work as described earlier. This assures that everyone is on the same page regarding what is being evaluated and how it will be evaluated. Once the audit is complete, there should be a report of findings that identifies the outcomes. If there are any issues identified that need corrective action, there should be a direction of the business unit management to prepare a response with a plan on how they will address the issues. To help ensure that corrective action is identified and implemented, the business unit should be required to produce their corrective action plan within a defined time and have defined timelines for implementation and completion of any tasks in the plan.

There may be valid reasons for audit, review, or monitoring activities not being completed as anticipated.

An additional item to keep in mind is any determination that issues identified in a billing, coding, and documentation audit resulted in the identification of overpayments from third-party insurers or patients. This would trigger the need to refund money to the appropriate party. If the third party owed the refund is a government payer, the 60-day repayment rule may be implicated. This adds an additional time pressure and need for monitoring to ensure the repayments are made in a timely fashion.

For the monitoring activities, regardless of who is conducting them, an important factor is to ensure the activities are happening and documented. Generally, there should be identified consequences for monitoring activities that are not completed.

Documentation, documentation, documentation! It is an essential component for auditing and monitoring, as it is in any compliance function. There may be valid reasons for audit, review, or monitoring activities not being completed as anticipated. If that is the case, there should be supporting documentation to demonstrate there was an exception or change. If a business unit becomes short staffed for a period of time, the requirement to conduct monitoring may be temporarily suspended. Documenting this will help explain why there are no metrics for the period, and it can also demonstrate that the monitoring activity was not being ignored or that an employee was being negligent.

If the auditing work plan that was approved by the governing body needs to be adjusted, then it should be taken back to the governing body for them to approve any modifications. There may be a number of reasons that adjustment or changes are needed, such as an unanticipated, significant investigation, or changes in staffing levels due to resignations or unanticipated medical leave. Because the ultimate responsibility for risk tolerance is always with the governing body, they

need to be aware of why the approved work plan may no longer be realistic in the changing circumstance. This allows them to make decisions on whether to approve resources to allow the approved work plan to be completed or to decide that a risk that was previously being addressed is removed from the adjusted work plan.

Conclusion

Communication and documentation are critical to having effective auditing and monitoring in the compliance program. Engaging senior leadership and business unit leaders in the process helps assure their buy-in. Partnering with departments such as Internal Audit can help cover more risks in the ever resource-strapped healthcare organization.

Independence and objectivity are key to performing audits. Balancing auditing activity with monitoring activity may help take some of the burden off the Compliance Office while helping ensure high-priority risk areas are being addressed. Keep in mind the compliance officer oversees compliance, but risk tolerance decisions are the responsibility of the governing body. Staying focused on this may help the compliance team sleep better at night when the governing body makes decisions regarding risk that would otherwise cause stress and worry. Compliance's role is to help ensure leadership makes informed risk decisions, but the compliance professional many not always be comfortable with the level of risk the governing body is willing to tolerate. Don't sweat the decisions that may be less risk adverse than you would prefer. If it can be said that the leadership had all the information they needed to make an informed decision, job well done.

1. US Department of Health & Human Services, Office of Inspector General: Work Plan. Available at https://bit.ly/2fV7PUP