An inside look at compliance auditing and monitoring: Integrating government standards
Both monitoring and auditing are an assessment of operations and controls, according to Laurisa Riggan, CPA, vice president, corporate compliance and internal audit, Children’s Mercy Hospitals and Clinics. Speaking during a recent audioconference provided by HCPro, the publisher of SHCC, Riggan compared the two functions.

**Auditing** is a systematic and objective assessment, methodical in nature, and includes a well thought-out plan, and a written report, she says. “A retrospective audit typically looks at a defined time period with the report based on that period.”

Auditing requires that the person performing the work is independent of the activities they’re auditing in order to conduct their work freely and objectively, she says.

**Monitoring** is more of a quality-control spotcheck—“you’re looking at a snapshot of a moment in time rather than an extended period of time,” she says.

This provides a baseline to compare against down the road. Monitoring isn’t necessarily as structured as an audit, and, while you only want to conduct an audit once every couple years, monitoring should be conducted on a routine basis.

The two functions feed off of each other. “An analysis of your monitoring activities may indicate areas that you need to audit and, vice versa, your audit results will provide key areas that should undergo routine monitoring.” Riggan says.

Determining what to audit and monitor, however, can be an issue you’re struggling with. Here are two suggestions from Riggan:

- **Look at issues that have been reported through your compliance program.** “As you resolve something, you may want to identify and monitor relative to that issue so that your corrective action remains in place on an ongoing basis,” she says.

Perhaps your compliance staff can take this on, but Riggan says it’s often beneficial to have the department staff directly involved in the problem process conduct the monitoring so they can see firsthand how they’re doing before the compliance department receives reports.

- **Look at the Office of Inspector General Work Plan.** “Figure out which items apply to your facility and then find those that you have not yet evaluated either through an audit or a compliance investigation,” she says.

Once you have a feel for how you are doing, you can decide whether you can look at this issue less frequently or whether you need to dig deeper to find out whether this is a real compliance issue or some anomaly.

To access this kind of data, you need to befriend someone in your information services department, Riggan recommends. “With the right access, you can obtain any report you want from your system, break it down, and analyze it in a variety of ways.”

Once you’ve decided what exactly you want to audit/monitor, you need to **identify what data you’ll need and what analysis you’ll put that data through.** “Most likely, you’ll want to heed external and internal forces.

For example, external forces include fraud alerts, local medical review polices, OIG reports—resources that tell you what the norm is. Internal forces can include medical records, emergency room logs, operating room logs, and contracts.”

- **Implementing a standard methodology** can help ensure that your auditing and monitoring results get back to the people who need to know. “There may be numerous people involved, so a written policy can provide consistency and close the loop by getting the information back to the compliance department.”
Practical auditing and monitoring tips

Auditing and monitoring are among the most important parts of your compliance program—and probably the most complex. At the Health Care Compliance Association’s (HCCA) Compliance Institute, Sheryl Vacca, CHC, HCCA president, offered the following six tips to simplify this task and make it more effective for everyone in your facility:

• Do not create a plan with 30 indicators. “You’ll just make yourself frustrated and you won’t have created any value for your organization,” said Vacca. “You’re probably under-resourced so you’ve got to prioritize. The things you want to do are what you can do. You want to get the biggest bang for your buck.”

• Consider your competitors. Look at what your competitors are having problems with—you could be next, Vacca advised. It figures that if one facility is having a certain problem, the government is going to check whether other facilities in the area are having the same problem.

• Remember to think in your senior managers’ frame of reference. When it comes to sharing the results of your auditing and monitoring, “the last thing you want to do is report a bunch of demographics,” said Vacca. “You want to report the business risks—those with a strong impact on the bottom line and quality of care. That’s what senior management wants to know about.”

• Don’t forget about customer service. If someone gets a bill for services that he or she did not receive, are you prepared to handle that? You want to track your complaints and see whether there’s a pocket of one particular issue.

• Be careful what you document in your auditing and monitoring plan. If you already know something is a risk, you don’t need validation. “There’s no reason to create documentation the government can use against you,” Vacca said. Do remedial work on the problem, she advised, and then work the issue into your auditing and monitoring processes.

• Don’t keep a problem area isolated. Most likely, a problem in one area affects other arenas in your facility. Keep that in mind, Vacca said, when you consider your overall compliance plan.

The audit dilemma: Use internal staff or an outside firm?

The first decision you have to make when conducting a coding audit is whether an external firm or internal staff will perform it. There are many arguments in favor of either approach.

Three arguments for conducting audits internally:
1. Internal audits are more cost-effective.
2. Providers have more control over audits conducted internally.
3. Conducting audits internally ensures that the provider will always keep abreast of compliance issues. Using internal staff forces the organization to constantly be on the cutting edge of compliance.

Three arguments for using external audit firms:
1. Outside audits may appear more credible than internal audits.
2. They may be more objective. An argument can be made that an outside firm can come in with no preconceived notions about the staff, work product, or legal exposure.
3. External firms may be able to offer expertise that the provider does not readily employ.

Editor’s note: This story was adapted from an excerpt of the book, Coding Compliance: A Practical Guide to the Audit Process, by Ruthann Russo, JD, MPH, RHIT. Go to www.hcmarketplace.com/Prod.cfm?id=106 to order this book.
The internal auditor’s role in compliance

The roles of the compliance and audit departments often overlap. The two may even review several of the same areas. To prevent overlap and improve efficiency, it’s important for the two departments to coordinate their roles and projects.

Compliance officers should show auditors their list of the greatest compliance risks to the organization. The auditor can then take that information and build it into the audit plan, says James Rose, CPA, CISA, director of internal audit for Humana, Inc in Louisville, KY.

Several important differences
An internal auditor helps an organization accomplish its objectives by using a systematic, disciplined approach to evaluating and improving the effectiveness of business risk control and governance processes, according to the Institute of Internal Auditors.

The auditor looks at all the risks that could prevent an organization from meeting its strategic and financial objectives, while the compliance officer focuses on compliance and regulatory issues, says Rose. Regulators are often the compliance officer’s number one customer; internal auditors directly support the board of directors, typically.

Compliance reviews
The internal audit department independently and objectively reviews an organization’s compliance and ethics policies and procedures, says Rose. The Institute of Internal Auditors wants auditors to evaluate the effectiveness of the following features of an enhanced, highly ethical culture:

- Formal code of conduct
- Frequent communication of expected ethical attitudes and behavior by the influential leaders of the organization
- Explicit strategies to support and enhance the ethical culture of regular programs
- Several, easily accessible ways for people to confidentially report alleged violations of ethics code
- Regular declarations by employees and vendors that they are aware of requirements for ethical behavior
- Clear delegations of responsibilities for investigation and resolution of case findings
- Easy access to learning opportunities regarding ethics
- Regular reviews of formal and informal processes within the organization
- Regular reference and background checks

Risk-based engagement planning
Look at your organization’s current control structure, past data reviews, and any other relevant information to determine the greatest gaps, according to James Rose, CPA, CISA, director of internal audit for Humana, Inc in Louisville, KY.

Rose says auditors must look at the overall objectives of the company first in risk-based engagement planning. Next, auditors should identify the risks that might affect those objectives, operations, or resources.

Consider the probability of significant errors, irregularities, noncompliance, and other exposures when developing engagement objectives, says Rose.

Use the result of the risk assessment to evaluate the adequacy and effectiveness of controls for the organization’s governance, operations, and information systems, says Rose. This should include:

- Reliability of integrity of financial and operational information
- Effectiveness and efficiency of operations
- Safeguarding of assets
- Compliance with laws, regulations, and contracts

An inside look at compliance auditing and monitoring: Integrating government standards
Time for a huddle

When a problem arises, auditors gather the experts

When auditors need to fix a problem, they shouldn’t go it alone, a group of speakers told attendees during a session of the Catholic Healthcare Auditing Network’s (CHAN) annual conference. The conference took place from May 29 to May 31 in Orlando, FL.

Auditors can find better solutions more quickly than they would otherwise by bringing together the people closest to the problem, said Margo Garcia, manager of audit and consulting services with CHAN at SETON Healthcare Network in Austin, TX. Bringing hospital officials together can motivate them to solve a problem themselves and increase their trust in the auditor overseeing their work. “You can get people to write audit reports for you,” Garcia said. “And you’re not perceived as just the outsider who doesn’t know anything.”

When one or more control mechanisms in a given process fail, auditors have to find out why. Garcia and her fellow speakers said you can best find the reasons by having the people who run the process assess themselves in a group setting. They call this group activity a “control self-assessment” (CSA).

The four presenters at this session showed attendees how to prevent these group efforts from breaking down and turning into shouting matches where officials hurl accusations at each other. Hence the name of the session, “Control Self-Assessment Facilitation Techniques.”

“You’re basically getting people together who are involved in a process to see what they do.”
—Margo Garcia

The four presenters at this session showed attendees how to prevent these group efforts from breaking down and turning into shouting matches where officials hurl accusations at each other. Hence the name of the session, “Control Self-Assessment Facilitation Techniques.”

Audience participation

Attendees shared their experience with running control self-assessments. Before assembling a CSA group, check to see that you’ve got everything you need. Putting together a “CSA tool kit” can help you prepare for these meetings, said Kelli Nueske, director of audit services at Allina Hospitals & Clinics in Minneapolis. Think of all the things you may need to bring, such as pens, pencils, paper, magic markers, an easel for drawing, and anything else you can think of.

Have your group draw a flow chart of the process in question, Nueske said. This will help group members understand each other’s roles, she said. “Sometimes, they don’t know who passes off to whom.”

A self-assessment can focus on any issue. One auditor in the audience discussed a task force that her hospital assembled to deal with reimbursement denials.

The task force, formed as part of a CSA, included the auditor herself, a representative from the hospital’s managed care payer, and employees with day-to-day involvement in patient financial services, case management, and performance improvement. (Getting the people with day-to-day involvement on your team is crucial, another auditor said.) The denials task force presented its recommendations for reducing denials to the hospital’s chief financial officer, who approved them.

The setup

Auditors can convene a CSA workshop for any of the following reasons: if a problem emerges in one step of process, if a problem affects an entire organization, or if the auditor needs to examine the process as a whole. Preparing for the workshop will take the most time, Michelle Piranio, manager for CHAN’s audit and consulting services in Kansas City, KS, told listeners. And the most important part of preparation is getting upper-level officials to go along with your plan. “They’ll wonder why you’re taking their people offline,” Piranio said.
Opportunity knocks for controls review and testing

Five tips to help you manage the process

Limiting your auditing and monitoring plan to testing results is a lost opportunity. Evaluating the controls used to achieve desired results can often be performed simultaneously and will help you focus your results testing and help you identify the corrective actions necessary to address problems indicated by the testing results, says Vickie McCormick, an attorney at Halleland Lewis, Nilan, Sipkins & Johnson in Minneapolis.

Preliminary and advance controls identification and review may help you decide whether to proceed with the testing, and how to do it. What’s more, controls identification and review will produce more focused, effective, and efficient testing, says McCormick. She offers the following tips for controls review and testing:

1. Identifying controls
During your audit also check the controls for each of the standards being audited through testing, says McCormick. Controls can range from a checklist, to a stamp, to a sophisticated software program. Develop a tool so the operational staff can identify the controls for you before you begin the audit. However, also talk to frontline staff to find out how they are really doing the work when reviewing controls and auditing.

2. Reviewing controls
McCormick suggests using the following guidelines when reviewing controls:

- If controls appear adequate or strong, proceed with testing
- If controls appear absent or weak, consider one of these two approaches:

  a. Test after implementing corrective action plan to improve controls
  - Why should you test before appropriate controls are in place?
    - Recommendations will improve new controls
  - Will have to test again after controls are implemented to ensure they work
  b. Test prior to implementing corrective action plan to improve controls
  - Verifies problems and may help identify necessary controls. Think of it this way: Why develop controls until you know what they need to be on the basis of testing?

3. Choosing a testing size
The testing size needs to be meaningful, but based on the risk assessment and compliance exposure, says McCormick. Use the following examples as a guide:

  a. If risk assessment/compliance exposure is high, use the standard sampling size
  - Make sure you have an accurate understanding of the compliance exposure and requirements
  b. If risk assessment/compliance exposure is low, consider using a probe sample
  - Use a probe sample for a quick picture of whether the risk area requires additional resources
  - If probe sample testing indicates compliance, move on to other risk areas
  - If probe sample testing indicates non-compliance, dig deeper

4. Find and prioritize risk areas
Organizations may not have the resources and time to focus on every risk area. Use risk assessments, business risk management profiles, the OIG Work Plan, state regulatory environment, hotline cases, litigation, and your instincts, says McCormick.

5. Offer meaningful solutions
Understand how your organization operates. Learn its resource limitations so you can raise issues appropriately and add value to the organization, not just criticism, says McCormick.
Sampling techniques enhance compliance effectiveness

Organizations are training employees and physicians on correct documentation and coding, but they won’t know whether it’s working unless they sample the medical records, said Sandy Piersol, a senior manager with Deloitte and Touche in Philadelphia, at the Health Care Compliance Association’s Annual Compliance Institute in April.

To sample, review a subset of specific components, characteristics, or items, and then measure them against an expected result. Sampling includes chart reviews, billing and coding reviews, etc., says Piersol.

There are no clearly defined parameters to determine sampling methodology, said Darrell Contreras, a manager with Ernst & Young in Phoenix. But organizations should consider the purpose of the sample or the review objective, the universe that the sample comes from, population or sources of data, the size of the sample, and what they are going to do with the results.

Choose a sample size
Determine a sample size that will give your organization a good level of comfort, said Contreras.

Contreras and Piersol suggest using the following examples as guides:

1. Review a minimum of 10 claims for reimbursement per provider, representing a cross-section of outpatient and inpatient evaluation and management services.

Analysis: This works for monitoring, but if you’re trying to do a statistical sample, you will need a larger sample size to meet precision and confidence.

2. Review five inpatient and five outpatient claims per provider.

Analysis: This is very specific, but it may not be as efficient. The sample could get very large if you’re trying to use a statistically valid sample.

Evaluate the compliance culture
How entrenched is your compliance program within the organization? Sample the compliance culture to find out, Darrell Contreras told attendees in April at the Health Care Compliance Association’s Compliance Institute. Use these guidelines for your next compliance program evaluation:

- **Compliance officer**
  - Do employees know who the compliance officer is and how to contact him or her?

- **Code of conduct and policies and procedures**
  - Do employees know about the code of conduct?
  - Is the location of policies and procedures known and are they used for guidance?

- **Training programs**
  - Are problems addressed in training still occurring repeatedly?
  - Does post-testing indicate that your employees understand compliance?

- **Hotline**
  - Do employees know about the hotline?
  - Are they willing to use it?

- **Non-retaliation policy**
  - Do employees know about this policy and, perhaps most importantly, do they believe it? If not, why not?

- **Repayments**
  - Is documentation of overpayments available?
  - Is there a policy for making repayments or voluntary disclosures?
Creating the audit tool

The audit tool provides the means for recording the data element collection. An audit tool can be created in either electronic or paper format. The most important point to keep in mind is that the audit tool for each record reviewed must be preserved for at least six years—the statute of limitations period under the federal False Claims Act. This six-year period should begin at the latest possible date at which a claim could have been paid; in some cases, this is as much as one year after the initial claim was submitted. Therefore, it could be more than seven years from discharge. If information is stored electronically or optically, retention is easy.

The audit tool must contain a space or field for each data element collected. In addition, the audit tool should collect the data in such a way that it is possible to group like responses and quantify data elements. For example, if you are recording “documents that support coding changes” as a data element, each document should be assigned a number or letter that could easily be grouped for reporting purposes. Then the auditor can simply record the assigned number or letter.

It is not a good idea to have the auditor enter the name of the document. If an electronic audit tool is used, grouping the following entries for discharge summary into the same category would be impossible: “discharge summary,” “D/S,” “DC Sum,” “D/C Summary.” If your hospital uses an object-oriented program to design its own electronic format for capturing data, this will not be an issue. In most cases, these programs use drop-down boxes from which auditors choose. In addition, the online screen edits that can be built into such programs ensure consistency when reporting.

Rules for designing the audit tool

Whether the audit tool is paper or electronic, some rules should be followed when designing it.

These rules include the following:

- Design the form with the user in mind
- Design the form as simply as possible; omit unnecessary data or information
- Use standard terminology for all data elements, or provide definitions; label all information
- Include guidelines as necessary to ensure data collection or interpretation consistency
- Sequence data items logically, in relation to their source document or in the order of their capture.

Editor’s note: This story was adapted from an excerpt of the book, Coding Compliance: A Practical Guide to the Audit Process, by Ruthann Russo, JD, MPH, RHIT. Go to www.hcmarketplace.com/Prod.cfm?id=106 to order this book.

The OIG’s hints for preparing working papers

The Office of Inspector General uses the following factors when creating the content for writing its working papers:

- Purpose
- Attribute—the condition, criteria, cause, effect, and recommendation of a finding to which the working paper pertains
- Source of the information
- Scope—include the number of transactions examined and the relationship between the number examined and total transactions
- Results
- Conclusion
- Preparer’s identity and date
- Notes and other symbols—explain each symbol in the working papers.

Editor’s note: This story was adapted from an excerpt of the book, Guide to Compliance Auditing: Applying OIG Techniques and Tools, by Hank Vanderbeek, MPA, CIA, CFE. Go to www.hcmarketplace.com/Prod.cfm?id=843 to order this book.
Protect sensitive information with ‘rigorous’ attorneys

The compliance and audit department may handle all your investigations and audits. However, if your organization wants to keep the results confidential, turn to an attorney.

Generally, all attorney-client privileged communications are confidential. A company has some control over when and how much it can make public with attorney-client privileged information.

Privilege applies to any form of communication in which legal advice is exchanged, says Boston attorney Mike Kendall. This includes audits of billing practices, review of contracts, and counseling advice on certain operational measures.

Consider using outside council
Lawyers rendering legal advice in bonified attorney-client relationships can protect privilege. In-house lawyers can do this, but they often serve in an administrative capacity and cannot assert privilege, opposing counsel often claims. Outside counsel, on paper anyway, should direct the investigation, says Michigan attorney Lori-Ann Rickard.

Using privileged information
Compliance officers and in-house councils should send the attorney copies of documents as they investigate. Always open correspondence with, “pursuant to your request,” says Rickard. Write “attorney-client privilege” on it, too.

Organizations can’t use privilege to shield things that are not privileged. Nor can they assert that privilege applies to something when it doesn’t, says Kendall. Attorneys must make sure privilege is used in the most correct and ethical way.

Waiving privileges
There are benefits to waiving privileges in certain situations, as long as you fully understand what you’re doing, says Kendall. Organizations often waive privilege to show the government they are acting on good faith—that no crime has occurred. “Sometimes, that’s an effective way to dissuade the government investigation from going forward,” Kendall says.

There is very little basis to selectively waive privilege, he adds. Disclosing some information to the government to help it understand your situation is generally considered waiving privilege.

Others will claim entitlement to that information because you waived privilege.

None of your business
How to keep privileged information to yourself

Keep all privileged information confidential between the attorney and the client, says Mike Kendall, Esq., a partner with McDermott Will & Emery in Boston.

Always leave a paper trail. Once relationships are established, attorneys will send a memo to management indicating that they are gathering information for privileged purposes. They will instruct their clients to keep the information confidential. Inform employees about their role and the confidentiality requirements involved in gathering information, says Kendall.

Everyone in your organization should sign a compliance agreement, though you can’t prohibit employees from becoming whistleblowers. The agreement obligates your employees to report any problems, or else they risk discipline. Compliance team members should sign another confidentiality agreement; this, forcing them to keep all compliance investigations confidential, says Lori-Ann Rickard, Esq., a partner in the Law Office of Lori-Ann Rickard, PC in Grosse Point Farms, MI.
Assess your risk of HIPAA noncompliance

Tracking and fixing instances of noncompliance no longer cuts it. You need to take your efforts to the next level by determining your weaknesses before a mistake occurs. Auditing and monitoring for compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) can help your organization do that.

An internal audit team can help the compliance and HIPAA implementation team test the processes in place, says Laurie Radler, RN, a partner at Deloitte & Touche in Jericho, NY at the Annual National Congress on Health Care Compliance. Internal auditors safeguard protected health information (PHI), identify risks of improper uses and disclosures, discuss compliance with subject matter experts (SMEs), review HIPAA policies and procedures, and develop a foundation for understanding HIPAA compliance opportunities and risks.

Not your average audit
Compliance audits usually start with the outcome, says Radler. However, with a HIPAA audit you start by developing a plan for testing the processes in place around a certain procedure. This ensures that the controls are adequate to achieve the processes’ goals, says Radler.

Start by bridging the gap
Determine the controls that need to be tested by performing a risk assessment, says Tina H. Sernick, RN, JD, a manager with Deloitte & Touche. This will help you identify and control weaknesses that may cause breaches of security and violations of the privacy requirements. Also take a look at the privacy office structure and HIPAA implementation plans to address administrative functions, use and disclosure of PHI, individual rights afforded, and business associate requirements.

Put your processes to the test
Focus your audits on areas of vulnerability identified in the initial assessment, says Radler. Work closely with privacy officials and security experts to evaluate and test the effectiveness of the HIPAA implementation plan policies, procedures, and business processes, says Radler. Benchmark by selecting high-risk departments and reviewing their policies and procedures to determine whether there is a gap between them and HIPAA requirements.

Then create checklists to monitor compliance exposure. Refer to the HIPAA implementation work plans, the Office of Inspector General’s compliance guidance reports, statutes, and regulations.

Once you have found the risk areas, implement a corporate-wide ongoing self-evaluation process to monitor and validate the effectiveness of the program. Start by checking your implementation progress against established deadlines, reviewing electronic testing plans and results of tests, and running code scans to determine whether prohibited codes have been eliminated.

Need more copies? That’s easy

If you’d like to order extra copies of this special report, please use the coupon below or call customer service at 800/650-6787. Extra copies are $29 each.

❑ I’d like ________ copies. The price is $29 each.
❑ Payment enclosed.
❑ Please bill me. ❑ Please bill me using PO # ____________
Charge ❑ AmEx ❑ MasterCard ❑ VISA
Signature __________________________________________________________________________
(Required for authorization)
Card # _____________________________ Expires ____________
(Your credit card bill will reflect a charge to “Opus Communications.”)

Name & Title ___________________________________________
Organization ___________________________________________
Address _______________________________________________
City __________________________ State ____ ZIP ___ ________
Phone (       ) ____________ ____ Fax (       ) ___ _____________
E-mail  ________________________________________________________

Mail to: Opus Communications, a division of HCPro
P.O. Box 1168, Marblehead, MA 01945
Call: 800/650-6787  800/639-8511
Fax: customerservice@hcpro.com  www.hcmarketplace.com
E-mail: ______________________________________________________
Internet: R0001
Look for these elements during your audit

Organizations should include the following elements in their audit for the Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliance, according to Laurie Radler, RN, a partner at Deloitte & Touche in Jericho, NY and Tina Sernick, RN, JD, a manager with Deloitte & Touche:

Security

- **Administrative procedures.** Evaluate documented administrative procedures for the selection and execution of security measures that protect data. Also, manage the conduct of personnel in relation to the protection of data.
- **Physical safeguards.** Evaluate computer systems and related buildings and equipment for protection from fire and other natural environmental hazards.
- **Technical security services.** Evaluate the processes for protecting information and controlling individual access to information.
- **Technical security mechanisms.** Evaluate the processes in place that guard against unauthorized access to data that is transmitted over a communications network.
- **Electronic signatures.** If electronic signatures are in place, determine whether they are used on electronic documents to bind them to a particular entity.

Privacy

In your review, determine whether the policies and procedures cover the following areas necessary for HIPAA compliance:

- **Administrative**
  - Appoint a privacy official
  - Train employees on the organization’s privacy policies and general HIPAA requirements
  - Disclose and transmit member information
  - Monitor HIPAA compliance and address individual complaints about privacy violations
  - Take corrective action for violations
  - Address employee discipline

- **Use and disclosure of PHI**
  - Check that an individual has given the organization written permission to make a disclosure, if necessary
  - Identify appropriate uses of PHI
  - Distinguish routine and non-routine disclosures of PHI
  - Respond to PHI requests and disclosures
  - Restrict the disclosure of employee health information from the group health plan and address the plan document
  - Track disclosures as required
  - Determine whether authorizations are valid
  - Require minimum necessary use and disclosure, noting exceptions
  - Designate the record set for an individual
  - Address deleting all PHI from member information before disclosing the information outside the company
  - Obtain patient authorization for marketing and fundraising activities

Individual rights

- Require the organization to permit individuals the right to access, copy, and amend their PHI
- Require the organization to respond to requests for restrictions and disclosure
- Address accounting for individual PHI disclosure
- Address individuals’ requests not to be in a facility directory

Business associates

- Address business associate agreements
- Identify and maintain current lists of business associates
- Address noncompliance with business associate agreements
The problem
The four presenters at this session explored what would happen if hospital officials got together to find out why their institution incorrectly classified and billed some short-stay patients as inpatients. These patients should have been placed in the emergency room (ER), observation, or outpatient surgery categories, presenters said.

A group of volunteers drew a flow chart of the ER process, starting from the moment the patient enters the department. Following an examination, the ER staff either sends the patient home, to the inpatient unit, or to the observation wing. Staff members fill out a pink slip based on physician orders and containing the patient’s diagnosis and personal information. Then they fax it to patient registration, where the registrars change the patient’s status in the system.

At this point in the process, the presenters found three possible reasons for patients winding up in the wrong category: the ER physicians may have written unclear orders, patient registration may not have picked up the faxed copy, or the ER has no concurrent review process to double-check physicians’ diagnoses.

Whatever the reasons, auditors should make sure they understand them, said Dorri McGhee, manager of auditing and consulting with CHAN. “Clarify to make sure you hear what [group members] say.” You should expect a fair amount of conflict in these groups as well, McGhee said. Before people start pointing fingers, find out where the disagreement comes from, and push for consensus. “Build little agreements along the way.”

The mock CSA group at this session ranked the following solutions to the classification problem in order of priority:

- 100% concurrent review for short-stay patients
- Reduce ambiguity of physician orders
- Improved communication when orders change

To make the first change, the ER would have to increase its staff or redefine job duties. To make doctors’ orders easier to understand, the hospital would have to revise its ER forms to include inpatient and outpatient designations. The department would also have to hold an inservice for nurses and doctors, and revise the case management process.

Finally, the next likely step would entail a meeting with senior members of hospital management for their approval on an action plan, followed by a report outlining the steps in that plan. -m-