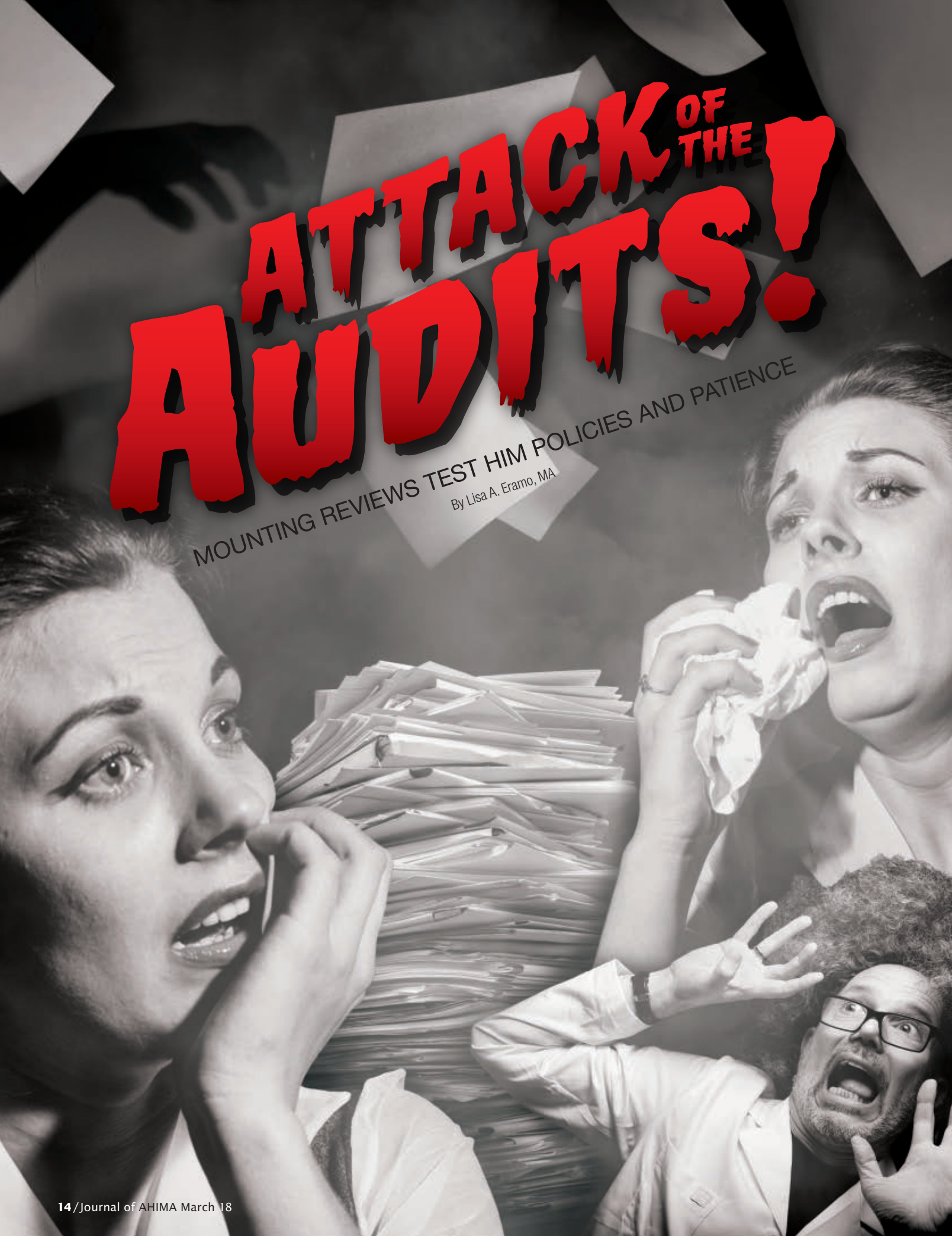

ATTACK OF THE AUDITS!

MOUNTING REVIEWS TEST HIM POLICIES AND PATIENCE

By Lisa A. Eramo, MA

THE RECENT ONSLAUGHT of audits in the healthcare industry, and the damage they leave in their wake, likely has many health information management (HIM) professionals fearing for the day audit requests storm their departments. Though audits may seem big and scary, proper preparation and the proactive adherence to best practices can protect and prepare HIM professionals.

Just as every story has two sides, so too is every audit a timeless tale of auditor vs. provider—and among those qualified to tell it is Elena Miller, MPH, RHIA, CCS, director of coding audits and education at Carolinas HealthCare System. Prior to joining the Charlotte, NC-based provider organization, Miller spent several years auditing claims for a Centers for Medicare and Medicaid Services' (CMS) Recovery Audit Contractor (RAC) and then a commercial payer. "It was always communicated to us during trainings that the purpose of the audit was to ensure accurate reimbursement," she says. "We were expected to make findings, but it was always for accuracy."

Now, tasked with handling all diagnosis-related group (DRG), coding audits and coder education at Carolinas HealthCare System, she admits that auditors sometimes send mixed messages. She provides the example of sepsis. An auditor might leave sepsis on the claim in one case but then deny the diagnosis on another record using the same criteria.

Carolinas HealthCare System has addressed this frustration by creating diagnosis- and denial-specific templates and checklists that staff can use to expedite appeals—particularly those that seem to contradict long-standing coding guidelines. These templates include all supporting *Coding Clinic* references as well as references to the *Medicare Program Integrity Manual*. Miller is also in the process of creating an internal library of payer-specific rules and policies.

Audits on the Rise with No End in Sight

Experts agree that when it comes to audits, the best defense is a good offense. This means HIM professionals must prepare proactively to address the inevitable frustrations associated with audits. And it's not just payer audits of DRGs, fee-for-service payments, and risk-adjusted reimbursement. RACs and other auditors are on the hunt for improper payments. The Office of Inspector General (OIG) investigates ongoing compliance vulnerabilities, many of which relate to coding and billing. CMS audits the documentation of how hospitals and eligible providers met the measures and objectives to support "meaningful use" Electronic Health Record Incentive Payment Program attestations that yielded financial incentive payments. But not all audits are about reimbursement. The US Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) audits covered entities' (CE) compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules and breach notification requirements. Then there are the internal audits conducted by healthcare facilities themselves to ensure the bills they send out the door include proper coding, and that coding professionals are up to par on productivity.

Over the last decade, these audits have continued to increase for a variety of reasons. Healthcare fraud and abuse is one of them. Others include an uptick in cybersecurity incidents and breaches, a continued disconnect between physician documentation and ICD-10 specificity, and the rise of clinical documentation improvement programs that may falsely inflate patient severity and risk.

Why should every organization pay attention to audits? The answer is simple: Unfavorable audit results jeopardize an organization's financial viability and possibly even its reputation. Costly recoupments, for example, place a financial strain on what has become an extremely slim operating margin. In addition, payers often consider audit results during contract negotiations. When audits reveal a pattern of high-cost outliers or non-compliant billing, providers are at a bargaining disadvantage. Any organization under the watchful eye of OIG must fear the public relations nightmare associated with publicly announced enforcement actions. Now more than ever, it behooves HIM professionals to give these audits the attention they deserve by turning frustrations into opportunities for proactive compliance.

Easing the Administrative Burden

Having a centralized approach can help organizations combat some of the administrative burden associated with audits, says April Carlson, MBA, HCISPP, CFE, privacy officer at Mayo Clinic, based in Rochester, MN. When one of Mayo Clinic's health system sites was randomly selected for an OCR HIPAA desk audit in July 2016, having a centralized approach helped the entity comply within OCR's 10-day timeline. More specifically, Carlson was listed as the privacy contact for all Mayo Clinic locations. When she received the audit request for its La Crosse, WI site, she immediately contacted the site's regional privacy officer and worked with a dedicated senior privacy analyst to coordinate with other departments and collect the required documentation (i.e., Notice of Privacy Practices, breach notification letters, policies/procedures, and more). "The three of us blocked our calendars for one week to allow time to retrieve, review, and redact PHI [protected health information], and submit the required documentation by OCR's deadline," recalls Carlson.

Carlson also took other preventive steps to expedite the audit process. For example, she created a centralized file storage location utilizing Mayo Clinic's secure SharePoint site so she could store, access, and share audit protocol information with all privacy officers across the organization. She also recommends working with the information technology department to prevent OCR emails from being blocked or flagged as junk to ensure any important correspondence is not overlooked.

Centralized audit management is critical, says Erin Head, MBA, RHIA, CHDA, CHTS-TR, director of HIM, quality, and medical staff services at Parrish Medical Center, based in Titusville, FL. At Parrish Medical Center, the compliance department receives all correspondence requests and then sends those requests to appropriate departments (primarily HIM). "We communicate to all of the potential auditors to use this contact to ensure we receive the request and have adequate time to respond. Otherwise, mail can get lost in the shuffle throughout the organization," Head says.

Addressing Inconsistent Audit Findings

As Miller alluded to in the sepsis example above, audit findings aren't always consistent or clear. This includes OCR's latest round of HIPAA Phase 2 desk audits, says David Holtzman, JD, CIPP,

Results of OCR's HIPAA Phase 2 Desk Audits

THE OFFICE FOR CIVIL RIGHTS'S (OCR's) overarching goal in conducting Phase 2 desk audits was to uncover vulnerabilities and detect areas for technical assistance—not penalize covered entities (CE) and business associates (BA), says Zinethia Clemmons, MBA, MHA, RHIA, PMP, HIPAA compliance audit program director at OCR. The Phase 2 audits concluded in December 2017, and Phase 3 is still in development, she says.

"As a result of Phase 2, we are going to publish a public report to share our findings and provide the industry with best practices," Clemmons says. The report will also go into more detail regarding the scope and methodology of the audits, including types of providers audited (i.e., labs, hospitals, or solo practitioners). OCR hopes to finalize and disseminate the document sometime this year.

Drawing from its own breach database and other sources, OCR used random sampling to audit a total of 207 CEs and BAs. Using a five-point rating scale, entities were assessed to determine whether their documentation—policies, procedures, sample notices, and breach notification letters—demonstrated compliance in seven categories:

- Content of breach notification
- Content of the Notice of Privacy Practices
- Provision of the Notice of Privacy Practices
- Right to access protected health information
- Security risk management
- Security risk analysis
- Timeliness of breach notification

Some notable preliminary results specifically for CEs as of press time include:

- Sixty-five percent of CEs had documentation indicating timely procedures for breach notifications (scored a 1); however, overall, the actual content of breach notifications required improvement 60 percent of the time (scored a rating of 2, 3, 4, or 5).
- Nearly all CEs (98 percent) needed to improve the content of their Notice of Privacy Practices (scored a 2, 3, 4, or 5).
- Nearly all (99 percent) of CEs needed to improve their documentation of processes for patient right to access (scored a 2, 3, 4, or 5).
- No CEs had policies and procedures of a risk analysis process that completely met the goals and objectives of selected standards and implementation specifications.

It's important to point out that the desk audits provide one view of compliance, Clemmons says. In some cases, policies may exist, but entities may not be following them. In others, compliant staff procedures might not be formalized through policy. "With an onsite audit, we're able to see whether entities are really doing what they say they are doing," she says.

April Carlson, MBA, HCISPP, CFE, privacy officer at Mayo Clinic in Rochester, MN, provides the following lessons learned after having been through a Phase 2 desk audit:

1. Use the Notice of Privacy Practices template and security risk assessment tool that HHS provides.
2. Ensure that the link to the Notice of Privacy Practices is visible. For example, consider enlarging it and making it bold on your organization's homepage.
3. Provide patients with specific options on the release of information form (i.e., email, print/mail, patient portal, or encrypted CD).
4. Think "specificity" when notifying patients of a breach. "Clinical information" is too vague. Include "lab results" or "surgical notes" instead.

To view the results and learn more about the OCR audit rating scale, visit www.nist.gov/sites/default/files/documents/sanches_0.pdf.

vice president of compliance strategies at CynergisTek. See the sidebar above for more information about audit results.

"OCR focused on issues that represented a very restrictive view, especially in its reviews of the security rule that allows covered entities a lot of flexibility in their approach to compliance based on the size and complexity of the organization," says Holtzman, who has personally seen several audit reports from organizations that have gone through an OCR Phase 2 HIPAA desk audit. "None of that flexibility was reflected in the analysis by OCR."

Carlson agrees that OCR seemed to go beyond what HIPAA requires. For example, although Mayo Clinic provides patients the right to access information in the format of their choice, OCR pointed out that they didn't spell out each option (i.e., encrypted email, print/mail, patient portal, or encrypted CD) on their authorization form. The organization is now in the process of adding check boxes on its release of information (ROI) form so patients can designate specifically how they want to receive information. If patients don't check a box, Mayo Clinic will default to paper mail.

Audit findings related to the content of breach notifications also seemed to go beyond what HIPAA requires, Carlson says. She provides the example of notifications specifying that demographic information was breached. OCR said these notifications weren't specific because they didn't describe the specific type of demographic information that was breached (i.e., name, address, or date of birth). "I think they expect to see more detail for the affected patient in terms of what was accessed or disclosed rather than being general," she says.

Streamlining Internal Audits, Coder Education

Although it creates more work for HIM, experts agree that internal coding audits may ultimately help reduce the external ones. At a minimum, organizations should plan and budget for quarterly internal audits—particularly if they're not already performing pre-bill DRG validation audits, says Kelly M. Carovillano, RHIA, vice president of client operations at Pena4.

Quarterly audits are important because coding guidance is

updated just as frequently. If organizations wait until six months or a year has elapsed before conducting an audit, there could be months of potential errors that go unnoticed, says Eileen Dano Tkacik, vice president of operations and information technology at Pena4.

Organizations should also supplement these audits with ongoing coder evaluations, ideally using software that provides coding professionals with immediate feedback and allows managers to drill down into knowledge gaps, Tkacik says. Doing so helps target coder education and allows organizations to develop internal edits and flags to check for errors before a bill is dropped.

It's also important to ensure that denials and education go hand-in-hand, Miller says. At Carolinas HealthCare, patient financial services used to handle all inpatient denials. Now, Miller oversees these denials and plans coder education accordingly. "I can see what denials are coming in first-hand and turn that into education fairly quickly and get it back to our coders," she says.

Internal audits help identify compliance problems before auditors do, thereby circumventing costly recoupments, Head says. "I believe we should be performing our own continuous assessments to look for compliance prior to being externally audited," Head says. "Coders should participate in ongoing education to stay on top of guidelines and changes, and internal audits should be performed regularly to ensure compliance."

There are plenty of resources that can help HIM professionals get the most "bang for their buck" in terms of internal audits. On the coding/billing side, resources such as payer denials, the annual OIG Work Plan, RAC targets, and a hospital's own Program for Evaluating Payment Patterns Electronic Report (PEPPER) are all goldmines of information that can help structure audits internally. PEPPER summarizes provider-specific Medicare data statistics for target areas often associated with Medicare improper payments due to billing, DRG coding, and/or admission necessity issues. TMF Health Quality Institute, under contract with CMS, began providing PEPPER to providers in January 2010.

On the HIPAA side, OCR's audit protocol can essentially serve as a blueprint and checklist for internal HIPAA compliance audits, Holtzman says. "The real value in the OCR audit program was the development of the audit protocol that, for the first time, provides organizations with insight into what OCR believes are measures for performance of the rules," he says.

Leveraging Data Analytics

It's not just about the frequency of audits, however—it's about performing audits that are most significant for your facility, says Miller, who works with an internal data analyst to plan focused audits in advance for the entire year. "If I think there's a topic that we need to look at, the analyst is easily able to get the data to help me decide whether we need to audit," Miller says. "It was better than 15 years ago when you didn't have the data and were just spinning your wheels. I'd rather have the data than randomly picking topics that weren't appropriate for our facility."

Carovillano agrees that analytics make audits more meaningful. "In the absence of a robust data analytics program, an HIM director may end up spending a great deal of time trying to make sense of the issues that may exist within the data," Carovillano says. "Using robust analytics to understand where opportunities for improvement exist is critical in ensuring your documentation and coding can stand up to any external auditor."

In the future, organizations may even start to team up and share data to address payer denials and audits, Tkacik says. "There's so much leveraging that can occur," she adds.

Head uses analytics to mitigate risk with "meaningful use" audits. "We validate all of the abstracted and coded data prior to submission to CMS," she says. "We do a sweep of accounts using data analytics to make sure everything is coded and validated prior to uploading our data to CMS so that we can mitigate any potential fallouts and mistakes."

When Auditors Give You Lemons…

…Make lemonade, says Carovillano. For example, coding audits can reveal costly coding errors, documentation problems, or chargemaster omissions. "For sure audits are frustrating; however, it is very true that they are sometimes the single driving force behind effecting any change towards documentation or process improvement in an organization," she says.

Carlson agrees that audits come with a silver lining. "We completely revised our Notice of Privacy Practices as a result of the audit," she says. "I do feel strongly that it is going to be better for our patients. It's easier to read and understand. That's one very positive thing that came out of this. It made us revisit the documents we felt complied with the rules, but weren't necessarily user-friendly for our patients."

The OCR audit also revealed an underlying systemic compliance issue with Mayo Clinic's ROI vendor. As Carlson and her team pulled records for the audit, they discovered that the ROI vendor wasn't sending a 30-day extension letter when necessary.

"Once we identified the issue we had it fixed within a day," Carlson says. "It was an important reminder that we needed to have better vendor oversight. It allowed us to find an issue that we probably still wouldn't have known about had we not been audited." Mayo Clinic now has a more defined quality oversight process in place with its ROI vendor to ensure they're sending the 30-day extension letter, charging the correct fees, and more.

"Really, it's about the patient," Carlson says. "We want our patients to be protected, and we want them to have the rights that they're entitled to. If we all do a better job, that's what's going to benefit patients in the end." ○

Lisa Eramo (leramo@hotmail.com) is a freelance writer and editor in Cranston, RI, who specializes in healthcare regulatory topics, HIM, and medical coding.