Year of the Audit

Save to myBoK

By Chris Dimick

The healthcare forecast for 2010 includes a strong chance of audit. HIM professionals in many organizations will be busy responding to a shower of external record requests and internal compliance checks.

Stormy systems of audit programs, compliance initiatives, and fraud prevention have been marching toward the HIM department over the past months. This year they will converge, raining down medical records requests, stinging audits, and high pressure reviews upon HIM departments. HIM professionals are facing more audit and compliance initiatives than ever before, say several industry experts.

HIM professionals will feel the impact in three main areas: coding, privacy and security, and fraud and abuse. Several new and revised private, state, and federal coding audits; privacy and security compliance audits; and amped up antifraud initiatives are likely to increase the amount of work for HIM professionals this year. In addition to the external audits, HIM departments will be conducting more internal audits to ensure they are prepared.

Coding Audits

This year is a high watermark for coding initiatives and audits. By one count there are 10 audit and fraud prevention programs being conducted by the federal government and quality organizations. Add in private payer requests and in-house reviews, and HIM departments are busier than ever responding to audit requests.

Federal programs, however, are making themselves felt the most. “I feel like the intensity has risen [in federal audits],” says Wendy Coplan-Gould, RHIA, president of Health Record Services Corporation, based in Baltimore, MD. “There is much more scrutiny than there has been over the last five years.”

The reason is purely financial. In 2008 the Centers for Medicare and Medicaid Services (CMS) issued a report that the money it spent on benefits now exceeded its federally allocated financial resources. In other words, more money was going out in payments than coming in through tax dollars. In order to lower its costs, CMS devised several financial recovery divisions to catch overpayments and fraudulent claims, according to Rebecca Busch, RN, MBA, CCM, CHS-III, CFE, CPC, FIALCP, FHFMA, the CEO of Medical Business Associates.

For years coders have dealt with an alphabet soup of federal audit programs: CERT, MAC, MIP, and PERM are just a few. But one new program tops the list this year: RAC.

RACs in Full Swing

The newest coding audit program facing coders in 2010 is CMS’s Recovery Audit Contractor (RAC) program. Initiated through Congressional legislation, this year marks the deadline for RAC contractors to begin conducting audits in all 50 states.

RACs evaluate a provider’s claims data and medical records for possible overpayments or underpayments. If an overpayment is detected, providers must return the money immediately.

While not every facility will experience a RAC audit, each should be prepared, Coplan-Gould says. RACs conduct two types of audits: analysis of claims submissions and review of actual medical records. The records requests will look at medical records and documentation from various areas.

Since the RACs are paid based on a percentage of overpayments they discover, the auditors are highly motivated to find overpayments. In just the initial five-state pilot phase of the program, RACs recovered nearly $993 million.

HIM departments that undergo a RAC audit will find it difficult to juggle the auditor's demands with everyday work, Coplan-Gould says. Departments will find it difficult to maintain a rhythm that allows them to respond to and monitor the requests as well as do their regular work, she says.

With HIM departments devoting more time to external audit programs, routine processes may suffer. Coplan-Gould fears that internal coding data quality audits will halt or be severely cut due to the demands of external audits. Instead of running quality coding reviews, HIM departments may focus their record reviews on RAC-related errors.

HIM departments should conduct their own mock RAC audits, following the guidelines posted on their RAC coordinator's Web site, Coplan-Gould recommends. This will reveal weak spots, if any, and allow time to make corrections before a RAC audit is conducted. The monetary risk of noncompliance is too great to sit back and hope you don't get audited, she says.

Caution in Replying to Private Payer Requests

HIM experts believe that soon private payers will devise their own versions of the RAC program. These retrospective, post-payment audits could add even more audit issues for HIM in the next few years.

Busch recommends caution when replying to private payer audits. She has worked with HIM departments that have seen payers request medical records for the sole purpose of conducting studies they can use to renegotiate managed care contracts.

These audit requests are not covered by HIPAA, and HIM professionals should be leery about releasing records to any payer without an explanation of why it needs the documents, Busch says. Using due caution in this manner also will help prevent releasing records to individuals posing as insurers who will use the material to commit fraud, she says.

"This isn't an environment anymore that HIM can assume that if they get a request from a payer that it is for a traditional purpose," Busch says. "The request letter needs to be disclosing what they [payers] are collecting, what is the purpose for the request, what do they intend to do with it, and if they intend to disclose it to a third party."

Privacy and Security Compliance

Privacy and security officials are equally tasked with new federal rules and a perceived increase in federal interest in enforcement.

The HITECH Act, passed in February 2009 as part of the American Recovery and Reinvestment Act, called for better enforcement of the HIPAA privacy and security rules. In August 2009 the Department of Health and Human Services (HHS) moved enforcement of the HIPAA security rule from CMS to the Office for Civil Rights (OCR). This placed both privacy and security under OCR for the first time, a move intended to coordinate efforts and increase enforcement.

This call to action and redelegation of enforcement duties has some in healthcare believing that privacy and security audits will increase and that OCR will take a more proactive role in enforcing the privacy and security rules, according to Tom Walsh, CISSP, president of Tom Walsh Consulting.

"There is greater coordination now in the follow-up when someone reports a privacy breach," Walsh says.

While OCR enforces HIPAA through fines and penalties, CMS still conducts the privacy and security compliance audits on healthcare organizations, Walsh says. He notes that at a meeting in Kansas late last year, a CMS official discussed how the organization was hiring auditors in order to ramp up healthcare privacy and security audits in 2010. During these audits, auditors compare an organization's written privacy and security policies against staff operations and the regulations.

HIM professionals should conduct their own internal reviews of their privacy and security regulations, Walsh says. An internal audit is the only way to know if processes are compliant with federal law.

The downfall of many organizations comes with the discovery that their written policies are nearly unachievable. The policy seems great on paper, but staff have difficulty following it in practice. An internal audit can spot these discrepancies before a federal auditor does and levies corrective action, Walsh says.

An organization that fails a privacy and security audit can be fined. If criminal behavior is detected, the case is turned over to the Department of Justice for possible prosecution.

With federal scrutiny increasing, Walsh recommends instituting self-audit programs immediately.

Is A**** a Bad Word?

Audit. Not necessarily an HIM professional's favorite word.

At its mention, HIM professionals, especially coding professionals, envision countless hours pulling and reviewing records, supporting intrusive visits from outside organizations, undergoing an evaluation of their job skills, and possibly losing revenue.

"I think it just causes the hair on top of the coders' heads to rise," Coplan-Gould says. "We are really uncomfortable with that phrase."

In fact, when conducting internal coding audits some organizations refrain from using the "A" word at all costs. The term can be adversarial to coders, who feel an audit means their work will be scrutinized for flaws and that retribution will follow.

Coplan-Gould says that at times clients request her company refer to its internal auditing service as "coding quality reviews" in order to ease staff.

Robertson understands coders' anxiety. "Audit" can suggest "you are not doing your job right-I am going to catch you on something," she says.

The difference between "audit" and "review" is subtle, Coplan-Gould says, but they can denote a difference. "Audit" should be linked to financial performance, she says, while "review" should be linked to quality performance.

For example, CMS may conduct a coding audit to ensure proper codes are being assigned and that correct reimbursement has been made. An HIM department or a consulting firm may conduct a coding review or assessment to evaluate a coder's selection of codes during a review of the record.

Regardless of what you call them, audits are necessary, says Robertson. Healthcare is a field blanketed in laws, and it is HIM's duty to ensure compliance. Further, internal audits are the only way to ensure that work is being performed properly.

"I don't find it a deterrent in any way. I think it is absolutely a sign of proving how good you are doing," Robertson says.

New Rules for Breach Notification

Add to the federal government's increased enforcement the new and modified privacy and security regulations resulting from the HITECH Act, and privacy and security officials have their work cut out for them in 2010, Walsh admits.

New provisions in the HITECH Act included expanded accountings of disclosure and additional rights for patient requests for restrictions. Facilities must conduct internal audits related to all these new policies to ensure they can meet compliance by the deadlines.

One of the biggest requirements HIM departments must meet now relates to breach notification. Beginning last month, penalties took effect for covered entities and their business associates that fail to meet federal requirements for notifying patients and the federal government when an unauthorized breach of unencrypted personal health information occurs. The new provisions increase a covered entity's responsibilities, and they could increase the potential for privacy and security audits.

"Before, the audits were ordered to be conducted by OCR based upon patient complaints," Walsh says. "Now they have a new source for going out and conducting audits, and that is through self-reporting when there is a breach."

Self-reported breaches offer OCR answers to the question "Where are we going to do our next audit?" Walsh says. Those facilities with a high number of reported breaches will likely be picked out by OCR and CMS for an audit, he predicts.

Facilities once again need to audit their breach notification processes and ensure they match the federal regulations. They must further ensure that safeguards are in place to prevent unauthorized disclosures of protected health information.

New Rules for Business Associates

The HITECH Act also extends HIPAA regulations to business associates, and covered entities can be held liable if their business associates fail to comply. Covered entities must ensure their partners are HIPAA-compliant, whether by requiring an external audit or conducting one themselves.

"The privacy officer needs to be on board, upfront, making sure that the agreements are in place," Walsh says, and determining in those agreements who will conduct the audit.

Federal HIPAA compliance audits are extensive and time consuming and include both records requests and site visits, Walsh says. In some cases, organizations can use up to 600 hours to support the audit. It is best to avoid the situation by taking the steps upfront through internal compliance audits, Walsh says.

Fraud and Abuse Enforcement

In recent years the federal government also has increased its resolve to fight healthcare fraud, and several new and revised programs are taking aim at Medicare and Medicaid abuse.

Last year, President Obama infused an additional $311 million into Medicare and Medicaid's fraud-fighting programs. Obama also signed into law the Fraud Enforcement and Recovery Act, which made it easier for CMS and law enforcement agencies to go after those committing healthcare fraud. The Health Care Fraud Prevention and Enforcement Action Team was revamped as an interagency program that works to improve existing fraud detection programs, using technology to stop fraudulent activity before payment is rendered.

These changes are bound to make 2010 a big year for fraud and abuse enforcement and auditing.

ZPICs: Scanning Claims for Fraud

One of the new fraud and abuse detection initiatives is the Zone Program Integrity Contractor (ZPIC) program, which becomes fully operational this year.

The RAC program looks mainly for administrative errors, and it is not specifically charged with rooting out Medicare fraud and abuse. That duty falls to the ZPICs, the aggressive cousins of RACs formed by CMS to detect fraudulent claims activity.

ZPIC was developed out of the Program Safeguard Contractors program, which was created in 1999 to detect fraud in the various CMS benefit plans. While the PSCs only searched for fraud in one benefit plan each, such as Part A, Part B, or Home Health, the ZPICs will search all CMS benefit plans for signs of fraudulent behavior.

The seven ZPIC contractors each cover a region of the country, scanning all claim submissions to CMS in that region for suspicious behavior. The ability to review all benefit plans at once gives the ZPICs a broader look at provider activity and will allow them to look for fraudulent submission trends that the PSC could not see, according to a CMS spokesman. For example,

ZPICs can look at billing trends and patterns, focusing on providers whose CMS billing services are higher than the majority of other providers in the community.

Once a ZPIC detects a potentially fraudulent trend in the data, it launches an investigation that requires providers to submit supporting medical records for their claims. If the records don't match the claims, the ZPIC refers the case to CMS, which can deny payment, suspend all future payments, and even revoke a provider's ability to bill CMS. If warranted, the ZPIC also will refer the case to the Office of the Inspector General for possible criminal prosecution.

ZPICs will also undertake investigations based on fraud tips that whistleblowers submit to Medicare as well as from referrals by CMS's claims processing contractors. Typically, ZPICs are going after blatant fraud, leaving administrative coding errors for the RACs.

"These are trained investigators, and we want them to focus on fraud, not just a clerical misunderstanding of correct billing practices," says Susan Oken, the ZPICs project officer at CMS. "There is too much fraud out there for us to spend time focusing our efforts on somebody that just doesn't understand the billing rules and can be educated by the MACs."

The first ZPIC was awarded in September 2008. CMS expects that by June 2010, all seven ZPICs will be operational.

Red Flags Rule

Medical identity theft is another form of fraud and abuse that harms patients and providers as well as payers. This June the Federal Trade Commission's Red Flags Rule takes effect, requiring businesses, including most healthcare providers, to implement and document identity theft prevention programs.

Though the rule's implementation has been delayed several times, April Robertson, MPA, RHIA, CHPS, FAHIMA, says that is not an excuse to delay compliance. "We know it is coming, so we should be working on it now," says Robertson, the vice president of customer advocacy at HealthPort.

Payer Fraud

While the federal government is trying to combat fraudulent payments, healthcare organizations also need to protect themselves from fraudulent behavior by patients and payers, Busch says. With bottom lines crashing and people losing insurance coverage in recent months, Busch says the amount of fraud will only increase throughout 2010.

"The provider market is often discussed as a perpetrator, filing false claims," she says. "But a provider is also a victim. Every market player can be a perpetrator or a victim."

Identity theft and patient fraud have taken their toll on providers. Developing solid antifraud policies and procedures is essential for healthcare facilities as they try to prevent becoming the victim of fraud themselves.

HIM professionals should audit their record release policies to ensure that they are not disclosing patient information to fraudulent payer organizations. "For HIM, the 'year of the audit' is about 'releasers beware,'" Busch says.

The act of a criminal posing as an insurer to obtain medical records is more prevalent than most HIM professionals think, Busch says. Typically, these fraudulent requests are submitted for the purposes of medical identify theft. HIM professionals should receive some training about how to detect fraudulent records requests.

"That is what makes HIM vulnerable-people who really understand how the department works and how correspondence works. They are writing letters in a typical format that is routine," Busch says. "So it is going to be really easy to miss letters that don't have altruistic intent."

Time to Shine

Today's audits require more resources. Past audits typically revolved around providing documentation that proved patients received services. Today, payers want proof that the services were warranted, Busch says.

Justifying services requires that HIM departments provide payers with more medical documentation. It also requires that HIM ensures the organization's documentation processes capture enough information for a medical record to tell the patient's story months after discharge. Busch expects this trend to continue.

HIM professionals can do more than just weather these new audits.

"It is the year of benchmarking," Robertson admits, but "it is also the year for HIM to shine and show how capable and how ahead they are in doing all this."

Chris Dimick (chris.dimick@ahima.org) is staff writer for the *Journal of AHIMA*.

Article citation:
Dimick, Chris. "Year of the Audit" *Journal of AHIMA* 81, no.3 (March 2010): 22-25:64.