Report on
Medicare Compliance

Volume 25, Number 7 • February 22, 2016

Weekly News and Compliance Strategies on CMS/OIG Regulations, Enforcement Actions and Audits

Contents

Cloning of Progress Notes, Upcoding Lead To Fraud Settlement; Doctors Pay $422,000

The cloning of electronic medical records has led to a fraud settlement, possibly for the first time.

Somerset Cardiology Group, P.C., in Somerville, N.J., agreed to pay $422,741 in a civil money penalty (CMP) settlement stemming from allegations it submitted false or fraudulent claims. The six-physician cardiology group allegedly cloned patient progress notes and upcoded evaluation and management (E/M) services, according to the HHS Office of Inspector General (OIG). The settlement was the end result of the cardiology group's use of the OIG Self-Disclosure Protocol, which it entered in August 2015. Attorney Joseph Gorrell, who represents the cardiology group, tells *RMC* that it discovered the alleged billing errors through an internal quality assurance process. "Once identified, a self-audit was performed, followed by self-disclosure," says Gorrell, with Brach Eichler.

Cloning refers to copying and pasting notes from one patient encounter to another without updating the information. Documentation is considered cloned if every entry in the record is worded the exact same way or it's very similar to previous entries. When entries are copied and pasted without being edited, this doesn't meet medical-

continued on p. 7

60-Day Rule Raises Question of Application To More Technical or Ambiguous Violations

It's a deeply unsettling thought: If provider-based departments have a minor technical violation — maybe they didn't give patients a perfect notice of copayment liability — hospitals could conceivably owe a lot of money under the final Medicare 60-day overpayment refund regulation published in the Feb. 12 *Federal Register (RMC 2/15/16, p. 1)*, one lawyer says. And maybe there would be the double whammy of their being unable to continue as provider-based departments because of Sec. 603 of the Bipartisan Budget Act of 2015.

That's one potential implication that attorneys are chewing over now that the regulation has materialized. It interprets Sec. 6402(a) of the Affordable Care Act, which requires providers to return Medicare and Medicaid overpayments 60 days from the day they are identified or from the date any corresponding cost report is due, whichever is later. Knowingly retaining an overpayment for more than 60 days may be pursued as a violation of the False Claims Act in what's known as a reverse false claim.

The final regulation, which has been welcomed by some lawyers for its clarity and flexibility, fleshed out the definition of "identified," with CMS stating that "a person has identified an overpayment when the person has, or should have through the exercise of reasonable diligence, determined that the person has received an overpayment and quantified the amount of the overpayment." That means they have to conduct a "timely, good faith investigation of credible information" about an overpayment, which

CMS says should take six months, absent "extraordinary circumstances." The look-back period is six years, so providers have to go back that far to quantify the overpayment, according to the final regulation.

Some aspects of the rule didn't sit well with attorneys, and that includes how murky areas of the law will be addressed. Washington, D.C., attorney Andy Ruskin says it's easy for hospitals to address a clear-cut duplicate payment, but what about ambiguous areas like provider-based compliance? "Think about the overlap of the 60-day rule and Sec. 603," says Ruskin, with Morgan Lewis. "What happens if your operations comply with the provider-based rule under one interpretation, but you know that some people at CMS or the Medicare contractor might disagree with that interpretation?" Sec. 603 put an end to newly created provider-based departments, although it grandfathered in existing provider-based departments, as long as they were billing the outpatient prospective payment system (OPPS) on Nov. 2, 2015, the date of the bill's enactment *(RMC 11/2/15, p. 1)*. There are reimbursement advantages to provider-based status because hospitals collect both a facility fee and a professional fee for services, while freestanding clinics collect only the professional fee.

If it turns out hospitals have run afoul of how CMS interprets the law, they may find themselves in a quandary about what to do under the 60-day rule, Ruskin says. For example, some CMS officials consider space noncompliant with provider-based rules if it's shared with freestanding clinics. One CMS regional office, for example, recovered a hospital's Medicare payments for provider-based services back to the date it had attested its compliance with provider-based status, and a major reason for the recoupment was the way the hospital shared space with an unrelated third party *(RMC 5/19/14, p. 1)*. That raises the question of whether similarly structured clinics would have to identify six years of overpayments when the final 60-day rule takes effect on March 14. If that's the case, it could be devastating for provider-based sites, which would have to calculate the difference in reimbursement for all services between freestanding and provider-based entities and repay that for the previous six years, he says. And questions could be raised about whether the spaces qualified for Sec. 603 grandfathering or are eternally banished from provider-based status, according to Ruskin.

"To what extent is CMS hoping to force hospitals to fall on their sword even though they have good arguments that an informal agency position — the CMS letter — does not necessarily result in a repayment obligation, but they would do it because they fear False Claims Act liability?" Ruskin says.

It's All About Risk Tolerance

Ruskin is not convinced that hospitals with technical compliance problems in their provider-based entities have a disclosure obligation as long as the hospitals rely in good faith on a sound legal interpretation of the regulation and related guidance. That would be true even when there's a contrary position in unofficial guidance, he says. "Although the 60-day repayment rule doesn't squarely address how to resolve reasonable differences of opinion between hospitals and individual staff members within CMS, repayments are due only for violations of law," he says. Obviously there will be close calls. "Is it enough to just have an argument that an entity is complying with the law? Or is it necessary to have the best argument before an entity decides not to disclose? For most entities, it will be somewhere in between," Ruskin says. "It's all a question of an entity's tolerance for risk."

The final Medicare 60-day overpayment refund regulation has other repercussions, attorneys say. For one thing, CMS is making it clear that "reasonable diligence" is part and parcel of an effective compliance program, says Boston attorney Larry Vernaglia, with Foley & Lard-

Report on Medicare Compliance (ISSN: 1094-3307) is published 45 times a year by Atlantic Information Services, Inc., 1100 17th Street, NW, Suite 300, Washington, D.C. 20036, 202-775-9008, www.AISHealth.com.

Managing Editor, Nina Youngstrom; Assistant Editor, Angela Maas; Contributing Editor, Francie Fernald; Executive Editor, Jill Brown; Publisher, Richard Biehl; Marketing Director, Donna Lawton; Fulfillment Manager, Tracey Filar Atwood; Production Editor, Carrie Epps.

Subscriptions to *RMC* include free electronic delivery in addition to the print copy, e-Alerts when timely news breaks, and extensive subscriber-only services at www.AISHealth.com that include a searchable database of *RMC* content and archives of past issues.

To order an annual subscription to **Report on Medicare Compliance** ($764 bill me; $664 prepaid), call 800-521-4323 (major credit cards accepted) or order online at www.AISHealth.com.

Subscribers to *RMC* can receive 12 Continuing Education Credits per year, toward certification by the Compliance Certification Board. Contact CCB at 888-580-8373.

ner LLP. According to the preamble, "The regulation uses a single term — reasonable diligence — to cover both proactive compliance activities to monitor claims and reactive investigative activities undertaken in response to receiving credible information about a potential overpayment. We believe that compliance with the statutory obligation to report and return received overpayments requires both proactive and reactive activities. In addition, we also clarify that the quantification of the amount of the overpayment may be determined using statistical sampling, extrapolation methodologies, and other methodologies as appropriate."

Between the lines of this provision is a warning that providers have to look for overpayments, Vernaglia says. "That's an expansion beyond the language of the statute under the 'should have known' language," he says. "It's another message to providers that they need to have an effective compliance program."

Many Reasons for Longer Investigation

Another provision that bears close analysis is the six-month investigation benchmark. It's not "an absolute cap," Vernaglia notes, and there will be "extraordinary circumstances" that take longer than six months to pin down (e.g., Stark violations). Other possibilities, he says, include "anything with significant statistical work, interviewing numerous or uncooperative witnesses, managing a large data set — something esoteric that requires you to identify the best experts [in the field], or sometimes you go down one path, and it takes a while before you realize you have to go down a different path," he explains. The six months for an investigation is "good for everyone — providers, the government and the public," says Vernaglia.

It's a relief to see a clearer definition of "identification," says attorney Bob Wade, with Krieg DeVault in Mishawaka, Ind. Whistleblowers will have a harder time rushing to argue that hospitals violated the False Claims Act when an overpayment wasn't returned the moment it's identified, as alleged in the case against former Continuum Health Partners hospitals in New York City *(RMC 8/10/15, p. 1)*. But hospitals can't drag their feet. "If a suspected overpayment is brought to the attention, usually of the compliance officer, you have a duty to review," he notes. "You can't just blow it off and say it's not credible."

And that will require an adequate budget for compliance and audit departments, says Wade. That's essential now that CMS extended the look-back period to six years. "It raises the complexity of doing reviews" — especially if there have been any software updates.

The final regulation muddied the waters with respect to cost reporting, says Washington, D.C., attorney Daniel Hettich, with King & Spalding. CMS said cost report overpayments should be repaid when hospitals file their cost reports with the Medicare administrative contractor (MAC) five months after the cost reporting period is over. But this rule is not as neat and tidy as it sounds, he says. For one thing, providers may wind up identifying overpayments after they file their cost reports but before the MAC has completed its audit many months (or years) later, he says. "Providers argued they should be allowed to wait for the audit to be completed before having to return those overpayments, but CMS said the mechanism for reporting the overpayment identified after the initial cost report is filed is filing an amended cost report, and suggested that the 60-day rule applies in these instances." It's normal for there to be numerous adjustments to a cost report, and now it appears that when providers become aware of them after filing their cost reports, they have an obligation to file an amended cost report or risk liability under the False Claim Act, Hettich says. "That's a big deal."

The Cost Report Conundrum

Other aspects of the 60-day rule pertaining to cost reporting trouble Hettich. For example, CMS has said the MAC's identification of an overpayment on a current cost report constitutes credible evidence of a potential overpayment on earlier cost reports and triggers the provider's obligation to do "reasonable diligence" during the six-year look-back period. Hettich wonders if that means every negative audit adjustment on the cost report creates an obligation to review prior cost reports for similar issues. The look-back period is irksome in this regard because CMS hasn't dealt with reconciling the six-year look-back period and the three-year cost-report reopening period, he says. One possibility: "CMS will expect repayments to be made off the cost report."

Also, Hettich questioned the fairness of CMS's policy when applied to issues of real controversy. For example, several courts have nixed CMS's policy that a hospital must look at a Medicare patient's assets and income to determine indigency for bad-debt purposes, yet this is still CMS policy, he says. So if a MAC denies bad-debt reimbursement for failure to apply an asset test in the current year, does the hospital have to request reopenings to return all indigent bad debts where an asset test wasn't used in previous periods? "CMS might say yes, but that would be pretty unfortunate and would effectively conscript hospitals to play the role of the MAC in determining that CMS policy might be applied to earlier periods," Hettich says. "It's like staring at a Jackson Pollock painting. What did Congress actually mean?"

Contact Vernaglia at lvernaglia@foley.com, Wade at rwade@kdlegal.com, Ruskin at aruskin@morganlewis.com and Hettich at DHettich@KSLAW.com. ✧

Protocol for Internal Investigations

This guidance for responding to internal compliance reports and conducting internal investigations was developed by Mark Pastin, president of the Council of Ethical Organizations in Alexandria, Va. Contact Pastin at mpastin@corporateethics.com.

Preliminary Analysis

When evaluating whether to initiate an investigation into an allegation of potential wrongdoing, the following issues are considered:

1. The nature of the allegation.
2. Whether a possible criminal matter is involved.
3. The scope of your authority in the matter.
4. Whether the issue merits a compliance investigation. If not, where and by whom, if anyone, should the matter be investigated?
5. The source of the allegation (e.g., employee, vendor, customer, competitor, etc.).
6. The manner in which Compliance became aware of the matter (e.g., the hotline, reported directly to Compliance staff, Human Resources, as a routine audit, risk assessment, potential litigation or a claim involving a compliance policy or procedure).
7. Who else may be aware of the matter.
8. Who should be notified? In matters of potentially significant consequence, the ordinary course would be to notify the CEO and the Board of Directors. In cases in which the CEO may be implicated, the Compliance Officer should immediately notify the Board of Directors or a designated member of the Board of Directors.[1]
9. Whether a government inquiry is underway or to be expected.
10. Who is (or may be) involved in the matter.
11. The potential impact of this matter on the organization (worst case scenario).
12. If there are any organizational obligations with respect to the issue (e.g., external reporting requirements, disclosures, insurance involvement).
13. Potential uses of the investigation findings.

If an internal compliance investigation is required, use answers to the above questions to prepare for the investigation.

Preparation

1. Document the allegation.
2. Develop an Investigation Plan. Part of the process of developing the Plan is to determine if legal privilege is appropriate. If so, Legal Counsel should participate in the development of the Plan and the execution of all later steps in the Plan.
3. Determine who should handle the investigation (Compliance Officer, an investigation team, other responsible executive, outside investigative resource).
4. Identify who will lead the investigation and the additional investigation team members (if any).
5. Assess whether those handling the investigation can devote the time necessary to complete the investigation and can proceed in an unconflicted (with their other ORGANIZATION duties) manner.
6. Assess what additional resources, if any, are required to conduct the investigation.
7. Identify any special expertise that the investigator(s) will require (e.g., legal, information systems, security, risk management, internal audit, accounting, etc.).
8. Establish a reasonable timeline for completion of each phase of the investigation. (It is generally reasonable to expect investigations to be closed within six weeks of the initial report date, but some investigations may take longer.)
9. Determine who will draft the investigation report and the timeframe for doing so.
10. Identify the policies/guidelines/regulations/laws/professional standards that may apply to the matter.
11. Identify background documents (including electronic records) for review (e.g., personnel records, emails, policies, procedures, meeting minutes, etc.).
12. Determine which documents (including electronic records) should be reviewed prior to conducting interviews.
13. Determine if there are documents that may be altered, removed, destroyed, or hidden and devise a methodology for securing them before there is knowledge of the investigation beyond the Compliance Officer and CEO or Board.
14. Identify who should be interviewed, by whom, in what order and in what setting.
    a. Person(s) who raised the issue (if known)
    b. Probable witnesses to any incident or set of circumstances
    c. Anyone suspected of having important, relevant information
    d. Any manager(s) who may have/should have known of the matter
    e. Person(s) suspected of being involved in potential wrong-doing
15. Determine whether special rules may apply (e.g., HR policies, contract requirements, federal/state/local

[1] If the Board does not want to be notified as a whole of pending compliance matters, a member of the Board (preferably an independent Director) should be appointed to serve as liaison between the Compliance Officer and the Board.

Protocol for Internal Investigations (continued)

law, regulations).
16. Prepare a list of areas of inquiry to be pursued and identify who will be responsible for getting answers to specific questions.

Implementing the Investigation Plan

1. Override document destruction schedules as appropriate. (This is a separate matter from protecting documents from intentional alteration or destruction, as above.)
2. Take steps to protect the confidentiality/privacy of information and individuals involved. If individuals additional to the Compliance Officer will participate in conducting the investigation, be sure to explain the confidentiality/anonymity conditions that apply to compliance investigations and gain their agreement to uphold these conditions (as opposed to those that may apply to investigations in their own areas of authority).
3. Gather all necessary material for investigation and protect in a secure location.
4. Review appropriate documents.
5. Conduct interviews with those who have relevant facts. Commit interviewees to maintaining confidentiality as to the content of the interview.
6. Perform document review, on site as required.
7. If others assist the Compliance Officer in conducting the investigation, obtain their reports. The Compliance Officer evaluates the adequacy of such reports and need for further investigation, if any.
8. Draft investigation report:
   a. Determine to whom the report should be directed (e.g., CEO, Board, legal counsel).
   b. Define a report distribution list (limit to "need-to-know" and limit ability to copy).
   c. Use office staff as little as possible to prepare the report; be sure office staff understand the need to maintain confidentiality.
9. Assess the investigation report:
   a. Mark "Confidential" or "Attorney Client Privilege" as appropriate.
   b. Identify by name and title members of the investigation team.
   c. Identify by name and title (if appropriate) those interviewed and documents reviewed.
   d. Provide key facts — not speculation.
   e. If opinion is appropriate, identify as opinion and provide the basis for the opinion. Limit opinions to those absolutely requisite to investigation follow up.
   f. Analyze all allegations raised and impact (if any) on the organization.
   g. Identify organizational policies/procedures, guidelines or laws that may have been violated (if any). Non-lawyers should avoid drawing legal conclusions.
   h. Reference all individuals identified as participating in the problem.
   i. Make recommendations on corrective action(s), discipline, etc. and state the basis for your recommendations.

The Corrective Action Plan

1. Determine if matter was an isolated episode or a systemic problem.
2. Determine what corrective action(s), if any, need to be taken.
   a. Modification to policies/procedures
   b. Modifications to training or additional training
   c. Disciplinary action(s)
   d. Government notification(s)
   e. Amendment to reports already submitted to regulatory agencies
   f. Refund of overpayments
3. Determine who is responsible for taking each corrective action and in what timeframe.
4. If additional resources are required to implement a corrective action, identify these resources.
5. State how implementation will be measured and monitored, duration of monitoring.
6. Re-evaluate the Compliance Program and modify as needed. Specifically, look at extent to which training and monitoring need to be fortified.
7. Identify opportunities to reinforce Compliance messages (non-retaliation, obligation to report, obligation to cooperate with internal investigations, investigation protocol, resources available, etc.).
8. Document steps taken in follow-up to the investigation.

Investigation Wrap-up

1. Notify person(s) who raised the matter, if appropriate, and provide such information as is consistent with confidentiality requirements. Reinforce non-retaliation policy and how to report perceived retaliation if this occurs. Remind reporter that retaliation is not always immediate and to notify compliance in any case.
2. Secure all records to retain confidentiality/privacy.
3. Follow up as indicated in the Corrective Action Plan and report implementation results to appropriate individuals.
4. Monitor corrective action(s) and report results as appropriate.

51 More Hospitals Settle ICD Cases; National Probe Comes to an End

Another batch of hospitals has settled cases over their billing for implanting cardiac defibrillators that allegedly were medically unnecessary, the Department of Justice (DOJ) said Feb. 17. Fifty-one hospitals in 15 states agreed to pay more than $23 million to resolve allegations they charged Medicare for procedures that did not comply with its national coverage determination (NCD 20.4) for implantable cardiac defibrillators (ICDs). A total of 500 hospitals have now settled with DOJ in connection with the six-year-long national ICD false claims investigation. Last fall, 457 hospitals in 43 states agreed to fork over $250 million *(RMC 11/2/15, p. 8; 10/5/15, p. 1)*. None of the hospitals admitted liability in the settlements.

The end of the enforcement initiative doesn't mean the risk evaporates. It clearly is on CMS's radar. The December 2015 release of the Program for Evaluating Payment Patterns Electronic Report (PEPPER) for the first time included data on ICD admissions *(RMC 11/23/15, p. 3)*, and Medicare administrative contractors are now looking at medical records for evidence ICD patients are in registries, which is an NCD requirement *(RMC 2/15/16, p. 1)*.

The ICD investigation kicked off in 2010, when DOJ sought coding, billing, denial and other information about the procedures from hospitals *(RMC 4/26/10, p. 1; 10/18/10, p. 1; 10/31/11, p. 1; 1/17/11, p. 1; 8/6/12, p. 1)*. ICDs are small electronic devices that shock the heart during life-threatening tachyarrhythmias (abnormal electrical activity), and hospital reimbursement for the procedure, which includes the device, runs $40,000 to $50,000.

The investigation focused on claims for ICD implantations that ran afoul of the NCD, which was last updated in 2005. According to the NCD, Medicare pays for ICD implantation for specific conditions, including:

(1) Cardiac arrest due to ventricular fibrillation (VF) that is not due to a transient or reversible cause.

(2) Documented sustained ventricular tachyarrhythmia (VT), either spontaneous or induced by an electrophysiology (EP) study, and not associated with an acute myocardial infarction (MI) and not due to a transient or reversible cause.

(3) Documented familial or inherited conditions with a high risk of life-threatening VT.

(4) Coronary artery disease with a documented prior MI, a measured left ventricular ejection fraction and inducible, sustained VT or VF at EP study (which measures the heart's electrical activity). Medicare coverage kicks in, however, only if the patient had the MI (heart attack) more than 40 days before ICD surgery. The EP test must be performed at least four weeks after the MI.

(5) Documented prior MI as long as certain circumstances don't apply (e.g., the patient had a coronary artery bypass graft (CABG) or percutaneous transluminal coronary angioplasty (PTCA) in the previous three months).

(6) Patients with ischemic dilated cardiomyopathy (IDCM), with other documented conditions (e.g., prior heart attack and heart failure).

(7) Patients with non-IDCM.

(8) Patients who meet all CMS coverage requirements for a cardiac resynchronization therapy (CRT) device and have class IV heart failure as designated by the New York Heart Association.

There is much more detail in the NCD, but one theme is Medicare's timing restrictions. In some of the categories, there's no ICD coverage within 40 days of a patient's heart attack or within three months of a CABG or PTCA. This is a source of frustration for hospitals and physicians because they contend the NCD is outdated. They are loath to play a waiting game when they think certain patients need ICDs immediately. But according to DOJ, "the medical purpose of a waiting period — 40 days for a heart attack and 90 days for bypass/angioplasty — is to give the heart an opportunity to improve function on its own to the point that an ICD may not be necessary." And all the hospitals that settled cases inserted ICDs during the periods forbidden by the NCD.

The case underscores the perils of overlooking NCDs and local coverage determinations (LCDs). "A lot of hospitals and physicians don't track LCDs or NCDs and don't really incorporate the latest pronouncements into their compliance programs, and it's important to do so," says Washington, D.C., attorney Jesse Witten, with Drinker Biddle. But he disputes the conventional wisdom that hospitals, by definition, commit fraud when they bill Medicare for procedures that don't satisfy all the

CMS Transmittals and *Federal Register* Regulations

Feb. 12 – Feb. 18

Live links to the following documents are included on *RMC*'s subscriber-only Web page at www.AISHealth.com. Please click on "CMS Transmittals and Regulations" in the right column.

Transmittals

(R) indicates a replacement transmittal.

Pub. 100-06, Medicare Financial Management

- Extended Repayment Schedule Manual Updates, Trans. 264FM, CR 9423 (Feb. 12; eff./impl. March 14, 2016)

Federal Register Regulations

- None published.

conditions of NCDs or LCDs. Citing the foreword to the *Medicare Manual on National Coverage Determinations*, he contends "they're more like a safe harbor for coverage." With the NCD for ICDs, for example, just because patients don't fall within one of the nine indications doesn't mean their implant isn't covered, according to Witten. It never expressly excludes coverage; there's just no guarantee, he says. In fact, he notes, the foreword states that if an NCD provides coverage of an item or service "for specified indications or circumstances but is not explicitly excluded for others, or where the item or service is not mentioned at all in the CMS Manual System, the Medicare contractor is to make the coverage decision in consultation with its medical staff, and with CMS when appropriate, based on the law, regulations, rulings and general program instructions."

There is difficult terrain at the intersection of enforcement and medical decision-making, Witten says. "A lot of hospitals have paid a lot of money to settle these cases, but I think every settling hospital settled for a lot less than they feared when they got an inquiry in 2010," he says. "They did a great job educating the Department of Justice about clinical issues and ambiguities in the NCD. These efforts caused government lawyers to be a lot more reasonable and understanding in the eventual settlement demands they made."

Contact Witten at Jesse.Witten@dbr.com. View the DOJ press release at http://tinyurl.com/z6meb95. ✧

MDs Settle Cloning Case

continued from p. 1

necessity requirements for Medicare coverage because documentation isn't specific enough to the patient and his or her experience *(RMC 3/25/13, p. 1)*.

According to the settlement, OIG contends that from Nov. 1, 2011, to May 31, 2015, Somerset Cardiology Group "cloned patient progress notes, as well as improperly coded and submitted for payment to Medicare fee-for-service E&M services that used current procedural terminology (CPT) code(s) to reflect a higher level of service than the cardiologists actually performed." As a result, the cardiologists received higher Medicare payments than they were entitled to, OIG alleged. The practice didn't admit liability in the settlement. Gorrell declined to comment further at the request of his client.

Cloning is one of the electronic health record (EHR) shortcuts that require auditing by hospitals and other providers *(RMC 9/7/15, p. 1)*. EHR shortcuts could set in motion claim denials and potential fraud allegations by OIG, Medicaid auditors and law enforcement agencies. Given the risk of fines in this area, EHR shortcuts belong high on every hospital's risk-assessment list, says Cassandra Andrews Jackson, compliance officer and HIPAA privacy officer for SBH Health System in New York City.

Cloning isn't by definition a problem, she says. It's efficient to carry forward some information, such as past family/social history. "You don't want to repeat it," she says. If the patient's father had a heart attack 20 years ago, that doesn't need to be written anew if there is evidence the physician reviewed and updated the previous information. "But this visit must reflect care that was provided today. There's a presumption that what you are billing is appropriate, and that the medical records will substantiate it," Jackson says. Auditors will ask for medical records, which should match what was billed; cloned records may not make sense when compared with the claims if, for example, an old note about a sore throat was copied into a new encounter about chest pain.

"If notes don't support what was billed, that's the first red flag," she says. "Auditors may ask for additional notes, and if they see a pattern where, across patients, there are multiple service dates where notes look exactly the same, you know providers are not doing their due diligence."

One attorney observes that the settlement agreement with Somerset Cardiology Group only alleges cloning and doesn't describe how information was cloned. The attorney, who wasn't involved in the case and asked not to be identified, says some information that isn't visit-specific can legitimately be copied from one record to the next. "In fact, in some circumstances, copy-pasting a prior entry can be a tool to improve the completeness and accuracy of the clinical record, rather than expecting a patient to remember and repeat every surgery or clinical episode or medication when asked each time he or she visits a practitioner," she says. CMS also has recognized the use of templates (*Medicare Program Integrity Manual,* Chapter 3, Sec. 3.3.2.1.1.), but providers have to tread carefully, she says. "If clinical findings, treatments and other information specific to a particular visit are not in fact from that visit but cloned from a prior visit or, even worse, from another patient's visit, obviously that is not an appropriate clinical or compliance practice. Such efforts could inflate claims or create fraudulent claims, and distort the patient's own clinical record," the attorney cautions.

To get cloning onto the audit agenda, Jackson suggests compliance officers take their case to their

compliance committee. "Hopefully it is populated with senior leaders of your organization," she says. "I think they have better understanding beyond the clinical environment of the potential cost to the organization if we don't assess and mitigate our risk in this area." The committees should do a risk assessment using the 14 "recommended requirements for enhancing data quality in electronic health record systems" set forth in a report by RTI International, a nonprofit institute, and a 2013 HHS OIG report on EHR fraud safeguards (OEI-01-11-00570). "It's best for us to get ahead of this," Jackson maintains.

And she wants to get the word out: Meaningful use is not a silver bullet, as some providers apparently believe. "As you assess vulnerabilities in the system, you should also realize that a certified EHR is not synonymous with fraud prevention," Jackson says. At this stage of EHR implementation, she notes, most hospitals are wedded to a specific EHR product. Making changes this late in the game is difficult, so the compliance committee has to press IT to make changes necessary to ensure fraud prevention. "The EHR implementation was based on the hospital's clinical workflows, and these will have to be reviewed to ensure that the workflow isn't contributing to the fraud risk," she explains. "The EHR product may or may not have certain fraud-prevention functions to mitigate the fraud risk."

Contact Jackson at candrewsjackson@uchcbronx.org and Gorrell at JGorrell@bracheichler.com. ✧

NEWS BRIEFS

◆ **In a case where a Medicare scam led to patient deaths, the owner of a Maryland diagnostics company was convicted of health care fraud and other charges,** the U.S. Attorney's Office for the District of Maryland said Feb. 17. Rafael Chikvashvili of Baltimore, who owned Alpha Diagnostics, a portable diagnostic services provider in Owings Mills, neglected to render medical services to patients who needed them and charged Medicare for services that he didn't provide, the U.S. attorney's office said. Alpha Diagnostics operated in Maryland, Delaware, Pennsylvania, Virginia and the District of Columbia, and its clients included nursing homes. Chikvashvili conspired with others to create false radiology, ultrasound and cardiologic interpretation reports and conveyed to Medicare and Medicaid that licensed physicians had interpreted diagnostic tests, the U.S. attorney's office said. In reality, he told nonphysician employees to interpret tests. "According to the testimony provided at trial, two patients died because their X-rays were not interpreted by a qualified radiologist," the U.S. attorney's office said. Nonphysician employees reviewed the images and failed to detect congestive heart failure. Chikvashvili was found guilty of health care fraud and wire fraud conspiracy; health fraud, including two counts of health care fraud resulting in death; wire fraud; false statements; and aggravated identity theft, and taken into custody immediately. In July 2014, Timothy Emeigh, the former vice president of operations for Alpha Diagnostics, pleaded guilty to health fraud in connection with the scheme *(RMC 7/21/14, p. 8)*. He is awaiting sentencing. Visit http://tinyurl.com/gl6nok7.

◆ **A Maryland chiropractor was sentenced to seven months in prison in connection with his guilty plea for obstructing a criminal health care fraud investigation involving Medicaid,** the U.S. Attorney's Office for the District of Columbia said Feb. 16. Rehman Mirza, who practiced in Suitland, will also be confined to his home for six months after his prison term. According to the U.S. attorney's office, Mirza was questioned by the FBI in connection with a home health scheme because he was writing prescriptions and plans of care as the ordering physician "even though he was not a physician and was not legally or medically qualified and could not determine whether the services were medically necessary." He allegedly denied any involvement with Medicaid and tried to influence his assistant's statements to the FBI, "encouraging and suggesting that she not be fully truthful," the U.S. attorney's office said. Visit http://tinyurl.com/zd3epln.

◆ **New Jersey physician Labib E. Riachi and two of his companies agreed to pay $5.25 million to settle false claims allegations** about a week after they were announced by the U.S. Attorney's Office for the District of New Jersey *(RMC 2/15/16, p. 8)*. Riachi and his companies, Riachi, Inc. and the Center for Advanced Pelvic Surgery, LLC, which are based in Westfield, allegedly billed federal health care programs for diagnostic tests that usually weren't performed, including anorectal manometry, an invasive diagnostic test, and electromyography. The false claims complaint also alleged the defendants billed for physical therapy services performed by unqualified personnel. Visit http://tinyurl.com/js8hsd4.

If You Don't Already Subscribe to the Newsletter, Here Are Three Easy Ways to Sign Up:

1. Return to any Web page that linked you to this issue

2. Go to the MarketPlace at **www.AISHealth.com** and click on "Newsletters."

3. Call Customer Service at 800-521-4323

If you are a subscriber and want to provide regular access to the newsletter — and other subscriber-only resources at AISHealth.com — to others in your organization:

Call Customer Service at **800-521-4323** to discuss AIS's very reasonable rates for your on-site distribution of each issue. (Please don't forward these PDF editions without prior authorization from AIS, since strict copyright restrictions apply.)