CCH Health Care Compliance LETTER

Volume 8, Issue 8 health.cch.com April 18, 2005

Letters to the Editor

The CCH Health Care Compliance team welcomes comments or questions regarding articles published in the CCH Health Care Compliance Letter. Send comments to Sharon Sofinski, Coordinating Editor, at sofinsks@cch.com. For more information about the CCH Health Care Compliance Portfolio visit our online store at http://health.cch.com.

Last-minute lessons for complying with the HIPAA Security Rule

by Catherine Hubbard, MA, Contributing Editor

Privacy officers and security officers must coordinate their efforts in order to achieve successful implementation of the HIPAA Privacy and Security Rules, according to Kirk Nahra, a partner with Wiley Rein & Fielding, Washington, D.C., and Marc Goldstone, a partner with Hoagland Longo, New Brunswick, New Jersey, who offered some last-minute lessons for complying with HIPAA.

In most cases, health care organizations will need both a security officer and a privacy officer, said Nahra, who emphasized that one person probably can not do both jobs. "The skill set you need to be a privacy officer probably doesn't make you a security officer," he said.

"It's going to be a very rare organization indeed that can appoint the same person and have that person do the job effectively," Goldstone emphasized. He added that appointing a privacy and security team will help prove due diligence. "It's going to be very hard to tell OCR [the Office for Civil Rights] that you complied with both the Privacy Rule and the Security Rule by appointing the same person to the same positions," said Goldstone.

Even before the HIPAA Security Rule, which becomes enforceable on April 20, most companies already had security practices in place. But they simply "let the IT people figure it out," said Nahra. Now they must comply with the Security Rule. "It's now a compliance requirement, not a best practice," he said. "You have to document and have policies and procedures in place," he added.

The Privacy Rule, enforceable since April 2003 for most health care organizations, requires covered entities to take scalable steps to ensure the privacy of personal health information (PHI), while the Security Rule is focused on implementing security specifications and securing electronic PHI in the most suitable manner, said Goldstone. "They require two different mindsets to implement," he said.

Complementary jobs. However, the two officers can complement each other, Nahra said, noting that the IT staff can figure out how to implement the policies and procedures and the privacy officer can manage risk, understand and translate the security measures and train employees on security procedures. "Privacy officers can manage the security process," reviewing a list of HIPAA process questions, the decisions the IT staff has made, the risks they've mitigated and those left unaddressed. "Somebody has got to sit down with the IT person and figure out what they've done and haven't done," he said.

The privacy officer is charged with creating a culture of privacy in the institution and communicating to employees the security measures necessary for compliance. Yet, it is up to the security officer to protect the systems from hackers and other security breeches. "The security officer is a person who's in charge of building the

moat," Goldstone said. "The person who says 'My secure, e-PHI is inside the moat and I've built a deep enough moat so that nobody can get in.'"

Employees may be accustomed to getting information out of the systems in the easiest way possible, but that is not necessarily the most secure way. "We need to make people understand that we need to do it in a way that's a little harder, but that's more secure," Goldstone said.

For instance, a major security threat is when employees write down their username or password for getting into a health care database system, Goldstone said. "It's clearly a security issue," he emphasized. The privacy officer needs to teach employees that "there are people whose reason for living is to get your password," he said.

Another growing threat is phishing, where people concoct a webpage or e-mail that mimics a financial institution in an attempt to trick victims into handing over their own or others' personal financial information. "The privacy officer is great at teaching about stuff like that. It might not be the security officer's forte," said Goldstone. In such an instance the privacy officer could alert employees and the security team to the problem and the information technology specialists could block the scurrilous e-mails. "That would be a great example of them working together," he said.

With only days before the HIPAA Security Rule becomes enforceable, health care companies are still struggling to implement the process-oriented rule, said Nahra. "There's no enforcement fear right now," he said in an interview. "Attention to the Security Rule is far less than that given to the Privacy Rule in terms of scope of effort, resources and management attention," he said.

Compliance lag. In addition, health care organizations have had a slower start in complying with the Security Rule, notes Goldstone. "The ramp up for privacy took so long and took so many resources, that it was an uphill battle to get to security," he said. "A lot of people were behind the curve," he said.

Even after organizations have reviewed their systems and taken all the reasonable steps to secure e-PHI, the job of their security officers will never be done. "It's a process," said Nahra, noting that the Security Rule does not provide a checklist, but a list of components the organization needs to consider. "Security is an evolution and you're supposed to consistently review what you've done," he said.

Furthermore, the goal of compliance is not to create a system without any risks. "I'd be astonished if anyone is fully compliant," Nahra said. "People may have different security procedures depending on their particular systems," he said. If something happens to one system, "it doesn't mean you've done something wrong," he said. "It means you've got some risk still out there." ■

CCH Washington Bureau, April 1, 2005

Risk assessment is critical to compliance with HIPAA Security Rule, CMS official stresses

by Catherine Hubbard, MA, Contributing Editor

A thorough risk analysis is one of the most—if not the most—critical parts of security implementation, according to Karen Trudel, deputy director of the Centers for Medicare & Medicaid Services' Office of HIPAA Standards. "That is the first thing we will look for," she said, noting CMS will focus on how thoroughly covered entities conduct their risk analyses. "The risk analysis is the key," she said, advising, "If the risk analysis hasn't been done, take the time to do it now."

Trudel suggested organizations resist shortcuts, such as buying off-the-shelf solutions for risk analysis or implementation of security provisions. "There is no getting around the value of doing a thorough risk analysis associated with the specifics of whatever covered entity you're advising," she told health lawyers during a March 24 teleconference sponsored by the American Bar Association's Health Law Section.

Voluntary compliance. Trudel also noted that CMS will focus on voluntary compliance of the Security Rule, which becomes effective April 20. "The enforcement for security will look very much the same as the process we already have in place for transactions and code sets and for privacy compliance," she said, adding that the process will be complaint driven. "The overarching goal of the enforcement process will be to achieve voluntary compliance," she stated.

CCH Health Care Compliance Letter

Managing Editor
Pamela K. Carron, J.D.

Coordinating Editors
Angela Fanelli, J.D.
Sharon Sofinski

CCH Washington Bureau
Paula Cruickshank
DOJ, FTC–John Scorza
SEC–Peter Feltman
Health Law–Catherine Hubbard
Tax–Jeff Carlson, Steve Cooper

Designer
Don Torres

Comments from readers are welcome and should be directed to Sharon Sofinski at SOFINSKS@CCH.COM, Tel. 847-267-7860, Fax 847-267-2514. Customer service inquiries should be directed to 800-449-9525.

CCH Health Care Compliance Letter is published 24 times a year by CCH INCORPORATED, 4025 W. Peterson Avenue, Chicago, IL, 60646. Subscription rate is $305 per year. First-class postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: SEND ADDRESS CHANGES TO *CCH Health Care Compliance Letter*, 4025 W. PETERSON AVENUE, CHICAGO, IL 60646. Printed in U.S.A.

Yet she emphasized that the enforcement process will be handled seriously. "We're serious about investigating complaints," Trudel said, noting that CMS has staff ready and procedures in place to handle complaints, including any complaints against CMS as a covered entity.

Custom security plans. Covered entities are challenged to implement security standards that are tailored to their individual needs, said Trudel. "We deliberately in coming up with these final standards did not address a cookbook solution. There is no out-of-the-box solution that you can buy to make yourself or your client HIPAA compliant," she said.

"This is not solely an information technology solution and buying information technology will not necessarily make your client compliant," she said, pointing out that about half of the requirements are administrative. "There are no shortcuts to doing a kind of individualized analysis that needs to be done," she said.

Do not overdo it. Health lawyers and covered entities should keep in mind that the security standards relate only to electronic protected health information, not PHI contained in paper records, Trudel advised. In the course of implementing HIPAA privacy, covered entities drew a perimeter around all of their PHI, not only electronic, but also paper and oral information. Thus, she said, if a provider does not use electronic health record systems in its clinical areas, the perimeter for HIPAA security may be centered on the billing office "and nowhere else."

"This is a really important concept," she stressed. "Skipping over that is going to cause some real problems."

Becoming unwired. Tom Kellerman, senior data risk management specialist with the World Bank's Treasury Security Team, Washington, D.C., discussed some specific gaps in security that many hospitals should address, particularly wireless communications. "Even the most secure e-security architecture can be compromised by the introduction of a [wireless network]," he said, noting that too many hospitals and doctors use unsecured wireless technologies. Calling WiFi the "weak link" in security of e-PHI, he said, "The wireless boom is compounding the security quagmire."

Even secured systems are vulnerable, said Kellerman. "Infesting public access points with trojans can undermine the most secure wireless devices," he warned. Trojans, he explained, create a rogue http tunnel and steal password information.

Preventing ID theft, the fastest growing crime, should be a priority, Kellerman said, noting a 3,600 percent increase in computer crime since 1997. Hackers use compromised routers and root access to services, party-to-party attacks, zip attacks and infected files downloaded from the Internet to gain entry into the systems, he said.

Managers need to be aware. "Lack of awareness can lead to negligence and liability," Kellerman cautioned. Managers need to understand the network topology, assume information is their responsibility, train employees and put a disaster recover and crisis plan in place, he said.

To build a more secure information system, said Ron Ross, with the National Institute of Standards and Technology, organizations need to:

- Develop an enterprise-wide information security strategy and game plan.
- Get corporate "buy in" for the enterprise information security program. "Effective programs start at the top."
- Build information security into the infrastructure of the enterprise.
- Establish a level of "due diligence" for information security.
- Focus initially on mission/business case impacts. "Bring in threat information only when specific and credible."
- Create a balanced information security program with management, operational, and technical security controls.
- Employ a solid foundation of security controls first, then build on that foundation guided by an assessment of risk.
- Avoid complicated and expensive risk assessments that rely on flawed assumptions or unverifiable data.
- Harden the target; place multiple barriers between the adversary and enterprise information systems.
- Be a good consumer—beware of vendors trying to sell "single point solutions" for enterprise security problems.
- Don't be overwhelmed with the enormity or complexity of the information security problem. "Take one step at a time and build on small successes."
- Don't tolerate indifference to enterprise information security problems.
- Manage enterprise risk: "Don't try to avoid it." ■

CCH Washington Bureau, April 4, 2005

Momentum building behind gainsharing

by Sanford V. Teplitzky and William T. Mathias

Despite setbacks in 2004, the momentum behind gainsharing is building in 2005. Last year, a federal district court in New Jersey blocked a CMS-sponsored gainsharing demonstration plan. This represented a significant blow to proponents of gainsharing. In February 2005, however, the OIG issued six advisory opinions approving limited cardiology gainsharing arrangements. See OIG Advisory Opinions 05-01, 05-02, 05-03, 05-04, 05-05, and 05-06. In March 2005, the Medicare Payment Advisory Commission (MedPAC) recommended that Congress approve broader gainsharing arrangements.

Background

It has been said that "when you've seen one gainsharing arrangement, you've seen one gainsharing arrangement." In fact, gainsharing covers a host of financial arrangements between hospitals and physicians designed to encourage physicians to use more cost-effective methods in delivering quality care in hospitals. Typically, gainsharing involves payments from hospitals to physicians for designing and implementing programs to control costs and to improve the quality of medical services provided to hospital patients. The payments can be structured in a number of ways, from hourly rates for services performed by physicians to a percentage of the realized cost savings.

Historically, physicians make decisions about the care provided to hospital patients, and hospitals provide the care. Under the Medicare prospective payment systems, hospitals generally receive fixed payments for different types of inpatient and outpatient services without regard to the hospitals' actual costs. Physicians are reimbursed separately based on fee schedules and thus have no financial incentive to minimize hospital costs. Interest in gainsharing has been growing over the years as hospitals try to reduce costs by aligning their economic interests with physicians through sharing cost savings with physicians.

In July 1999, the OIG stunned proponents of gainsharing when it issued a Special Advisory Bulletin taking the position that gainsharing between hospitals and physicians violates federal law.[1] Specifically, the OIG concluded that hospitals sharing cost savings with physicians constitutes a violation of the civil monetary penalty prohibition on hospital payments to a physician to induce reductions or limitations of patient care services to Medicare or Medicaid beneficiaries under the physician's direct care.[2] The OIG also noted that gainsharing arrangements potentially raise concerns under the anti-kickback law.[3]

At the time, the Special Advisory Bulletin was viewed by many as closing the door on most gainsharing arrangements, absent a change in federal law. In January 2001, however, the OIG opened the door to gainsharing a crack, when it issued an advisory opinion approving a narrow gainsharing arrangement.[4]

The OIG had very little to say about gainsharing for the next four years. In February 2005, however, the OIG issued six favorable gainsharing advisory opinions. While the issuance of these advisory opinions suggests a possible renaissance in gainsharing, caution is still warranted. The OIG found that virtually all of the elements of these six gainsharing arrangements implicated the CMP and the anti-kickback law. Nevertheless, in each advisory opinion, the OIG was able to identify sufficient protections to avoid imposing administrative sanctions against the respective gainsharing arrangements.

2005 Advisory Opinions

The analysis used by the OIG in examining these six recent gainsharing advisory opinions is identical to the analysis used in the gainsharing advisory opinion issued in 2001. However, the facts of the various gainsharing arrangements have some minor variations and the application of the OIG's analysis to the specific facts is instructive.

OIG Advisory Opinion 05-01 involved an agreement between a group of cardiac surgeons and a hospital, pursuant to which the group would share up to 50 percent of the hospital's savings arising from the surgeons' implementation of 24 cost savings recommendations in certain cardiac surgery procedures. The recommendations fell into four categories:

(1) opening certain packaged items, including disposable components of cell saver units, only as needed;
(2) performing blood cross-matching only as needed;
(3) substituting less costly items for items currently being used; and
(4) product standardization of cardiac devices.

OIG Advisory Opinion 05-02 involved an agreement between five cardiology groups and a hospital, whereby the groups would share up to 50 percent of the hospital's cost savings arising from the cardiologists' implementation of 18 cost reduction recommendations in certain cardiac catheterization laboratory procedures. The recommendations fell into two categories:

(1) product standardization of cardiac catheterization devices (stents, balloons, interventional guidewires and catheters, vascular closure devices, diagnostic devices, pacemakers, and defibrillators) and
(2) limiting the use of certain vascular closure devices.

OIG Advisory Opinion 05-03 involved an agreement between a group of cardiac surgeons and a hospital, in which the group would share up to 50 percent of the hospital's cost savings arising from the surgeons' implementation of 29 cost reduction recommendations in certain surgical procedures. The recommendations fell into four categories:
(1) opening certain packaged items, including disposable components of a cell saver units, only as needed;
(2) performing blood cross-matching only as needed;
(3) substituting less costly items (e.g., slush drape, wrist splints, armboards, aortic punches, or suture boots) for items currently being used; and
(4) product standardization of certain cardiac heart valves.

OIG Advisory Opinion 05-04 involved an agreement between eight cardiology groups and a hospital. The groups would share a maximum of 50 percent of the hospital's cost savings arising from the cardiologists' implementation of 17 cost reduction recommendations during certain cardiology procedures. The recommendations were grouped into three categories:
(1) product standardization of certain cardiology devices (stents, balloons, interventional guidewires and catheters, vascular closure devices, diagnostic devices, pacemakers, and defibrillators);
(2) limiting the use of certain vascular closure devices; and
(3) substituting less costly items related to contrast agents.

OIG Advisory Opinion 05-05 involved an agreement between a group of cardiologists and a hospital, whereby the group would share a maximum of 50 percent of the hospital's first year cost savings arising from the cardiologists' implementation of 12 cost reduction recommendations in designated cardiac catheterization laboratory procedures. The recommendations were grouped into two categories:
(1) product standardization of cardiac catheterization devices (stents, balloons, interventional guidewires and catheters, vascular closure devices, diagnostic devices, pacemakers, and defibrillators) and
(2) limiting the use of certain vascular closure devices.

OIG Advisory Opinion 05-06 involved an agreement between a group of cardiac surgeons and a hospital. Here, the group would share a maximum of 50 percent of the hospital's first year cost savings arising from the surgeons' implementation of 27 cost reduction recommendations in certain cardiac surgery procedures. The recommendations were grouped into four categories:
(1) opening certain packaged items only as needed;
(2) limiting the use of certain surgical supplies (e.g., gelfoam, surgical, and vancomycin paste) to an as needed basis;
(3) substituting less costly items (e.g., disposable head supports, disposable k-thermia blankets, and instrument pouches) for items currently being used; and
(4) product standardization of certain cardiac devices and supplies.

Each of the recent gainsharing advisory opinions included a product standardization recommendation. The OIG drew comfort in these advisory opinions from the fact that the individual surgeons would continue to make patient-by-patient choices as to the appropriate device and would have the same selection of devices as before the implementation of the gainsharing arrangements.

In those advisory opinions that involved either opening packaged items or substituting less costly items, the OIG concluded that the recommendations would have no appreciable clinical significance and thus would not implicate the CMP. One exception was for the items used with the cell saver units. For these, the OIG was concerned that the time it took for the cell saver units to warm up after the items were opened could have an appreciable clinical significance and therefore these items fell within the ambit of the CMP. Nevertheless, the OIG's finding that certain cost savings recommendations would not have an appreciable clinical significance suggests that hospitals may have greater flexibility in implementing gainsharing arrangements that focus on such savings.

Interestingly, a footnote in Advisory Opinions 05-04, 05-05, and 05-06 indicated that there were originally additional cost savings recommendations that were eliminated because they posed an unacceptable risk of fraud and abuse. This seems to reinforce the limited nature of the gainsharing arrangements approved in the advisory opinions and highlights the interactive nature of the advisory opinion process.

CMP Analysis

The OIG found that nearly all of the cost savings recommendations could induce physicians to reduce or limit the current medical practices at the hospital and thus implicated the CMP. While the OIG acknowledged that current medical practices at the hospitals may exceed what is medically necessary, the OIG found this fact irrelevant under the CMP. The OIG found that limiting medically unnecessary care could still violate the CMP. Nevertheless, the OIG found that the proposed gainsharing arrangements contained sufficient safeguards so that sanctions need not be imposed. The specific safeguards in each of the advisory opinions were as follows:

- **Identified Cost Saving.** Specific cost-saving actions and resulting savings were clearly and separately identified to allow public scrutiny and individual physician accountability.
- **Credible Medical Support.** Credible medical support existed for the position that the cost savings recommendations would not adversely affect patient care. In addition,

periodic reviews of any impact on clinical care would be conducted.

- **Limited Impact on Federal Health Care Programs.** Credible medical support existed for the position that the cost savings recommendations would not adversely affect patient care. In addition, periodic reviews of any impact on clinical care would be conducted.
- **Protections Against Inappropriate Reductions in Service.** Baseline thresholds would be established through the use of objective historical and clinical measures to protect against inappropriate reductions in services.
- **No Limits on Device Selection.** Savings from product standardization would be obtained from "inherent clinical and fiscal value." Individual physicians would continue to have access to the same selection of devices.
- **Patient Disclosure.** The hospital and the physician groups would provide patients with written disclosures about the arrangements.
- **Limits on Incentives.** Financial incentives would be reasonably limited in duration and amount.
- **Protections Against Disproportionate Cost Savings.** The physician groups distribute profits, and thus, any gainsharing payments, on a per capita basis, which should limit any incentive for individual physicians to generate disproportionate cost savings.

Anti-kickback Law Analysis

In analyzing the implications of the gainsharing arrangements under the anti-kickback law, the OIG noted that the arrangements would not satisfy the personal services and management contracts safe harbor. Specifically, the OIG noted that the payments to the physician groups were based on a percentage of the cost savings and thus the aggregate compensation would not be set in advance as required by the safe harbor. The OIG warned that gainsharing arrangements could be used to disguise illegal remuneration from the hospitals by encouraging physicians to admit more federal health care program beneficiaries to the hospitals. Despite the potential risk of illegal remuneration, the OIG declined to impose administrative sanctions based on several aspects of the gainsharing arrangements that suggested the risk of fraud or abuse was low.

- The circumstances and safeguards associated with the gainsharing arrangements reduced the likelihood that the arrangements would be used to attract referring physicians or to increase referrals from existing physicians: (1) the arrangements are limited to physicians on the medical staffs of the hospitals; (2) savings derived from procedures for federal health care program beneficiaries are capped based on the prior year's admissions; and (3) the arrangements are limited to one year.
- The structure of the proposed arrangements eliminates the risk that they would be used to reward non-surgeons for referring patients to the surgeon groups. Profits within the groups are distributed on per capita basis, which minimizes any incentive for an individual physician to inappropriately reduce services to achieve savings.
- The arrangements describe the particular actions that would generate the cost savings on which the payments are based. The physicians may have some increased malpractice liability risk from making the cost-saving changes for which it is reasonable to compensate them. Payments are limited in amount, duration, and scope.

MedPAC Recommendation

In March 2005, MedPAC issued a *Report to Congress on Physician-Owned Specialty Hospitals*. One of the five recommendations of the *Report* was that Congress should grant HHS the authority to allow gainsharing arrangements between physicians and hospitals. The *Report* recognizes the value of aligning the financial incentives of physicians and hospitals. Physician ownership of hospitals fully aligns their incentives. However, such alignments may raise concerns about self-referrals. The *Report* speculates that efficiencies could be achieved by allowing physicians to share in savings from re-engineering clinical care. The *Report* ultimately concludes that "[s]tructured properly, gainsharing arrangements could garner the benefits of aligning incentives while allaying legitimate concerns."

Conclusion

The OIG has drawn a distinction between generalized gainsharing arrangements tied to overall cost savings, which it views as prohibited, and limited gainsharing arrangements tied to specific, identifiable, and verifiable cost savings, which it may permit on a case-by-case basis. While the OIG has warned that the recent gainsharing advisory opinions should not be seen as throwing the door wide open to gainsharing, hospitals will almost certainly look to replicate these arrangements.

Given the relatively narrow scope of the advisory opinions, however, hospitals will have to carefully consider whether and how to implement gainsharing. First, hospitals will need to consider whether they can implement gainsharing without first obtaining individual advisory opinions in light of the OIG's assertion that the gainsharing arrangements that were approved through the recent advisory opinions violated the CMP and only the requesting parties are protected by those advisory opinions. Second, the recent advisory opinions express no opinion as to how, or if, gainsharing might be permitted under the Stark physician self-referral law. This is not unexpected given that CMS, not the OIG, is responsible for interpreting the Stark law. In any event, hospitals will need to carefully analyze any gainsharing arrangements for compliance with the Stark law.

While recent events have opened the door to gainsharing, the door is still just opened a crack. Without action by Congress to amend the CMP and probably the Stark statute, hospitals will continue to lack the tools necessary to effectively align their economic interests with physicians to control hospital costs.

[1] *Gainsharing Arrangements and CMPs for Hospital Payments to Physicians to Reduce or Limit Services to Beneficiaries* (July 1999), *reprinted in* 64 Fed. Reg. 37,985 (July 14, 1999).

[2] 42 USC §1320a-7a(b)(1) & (2) (the CMP).

[3] 42 USC 1320a-7b(b).

[4] OIG Advisory Opinion 01-01.

Sanford Teplitzky is a Principal and Chairman of the Health Law Department of Ober, Kaler, Grimes & Shriver and is resident in the Baltimore office of the firm. Mr. Teplitzky offers his experience to clients - typically large health care companies and delivery networks - who seek help with fraud and abuse problems and representation in federal or state investigations. He is a former president of the American Health Lawyers Association and a frequent writer and lecturer on various health care fraud and abuse issues. Mr. Teplitzky can be contacted at (410) 347-7364 or by email at teplitzky@ober.com.

Bill Mathias is a Principal in the Health Law Department of Ober, Kaler, Grimes & Shriver. He represents a broad range of health care businesses across the country with respect to fraud and abuse, corporate compliance, and reimbursement matters. He also represents health care clients in federal, state, and internal investigations and false claims cases. He can be contacted at (410) 347-7667 or by e-mail at wtmathias@ober.com.

Ethics

Coding documentation and ethics

by Catherine Hubbard, MA, Contributing Editor

Documentation is crucial to linking physicians and the healthcare teams that provide care, according to Karen Youmans, executive vice president of Pyramid Healthcare Solutions, St. Petersburg, Florida. It also links adequacy and appropriateness of patient care, links patient care to the payment, links individual patients to public health data and links clinical data to research and education.

Yet, many offices lack the thorough documentation required for coders to do their jobs correctly, including lack of timely information and poor communication between physicians and coding staff, said Youmans. "Bottom line, we need to educate physicians on what we need documented," she emphasized. She spoke during a March 3 American Health Information Management Association (AHIMA) audio conference on "Coding Documentation and Ethical Issues."

Youmans said medical record entries should be documented at the time service is provided, entries should be legible and authenticated, and subsequent additions should be identified as such and dated. "In the real world of Medicare, we know that this is not always a reality. We need to be creative in finding ways to make documentation easier as well as more accurate," she said.

Many physicians' writing is not legible, said Youmans. "Most physicians have attended Illegible Handwriting 101 in their first year of medical school and as they go through it gets worse," she quipped. Requiring physicians to type in key words may help coders obtain accurate information, she added.

Coders are challenged to communicate with physicians when clinical data does not correlate to the coding classification system, Youmans said, emphasizing that often the terminology used in everyday practice is different from that used in the code book.

Ethics in Coding. Laurinda Harman, associate professor and chair of the HIM program at Temple University, Philadelphia, Pennsylvania, said coders need to make the ethical decision not to upcode in order to bill more money to Medicare or to change a code in order to reduce a bill for a friend. "You as the coder ... can make sure you stay centered as a moral ethical agent," she said.

One of the ethical principles under the AHIMA Code of Ethics is that coders should refuse to participate in or conceal unethical practices or procedures, said Harman. "It's not enough that you code in an ethical way. If you know others who are not doing that, our Code of Ethics says you have to confer with them," she said. "We have to get involved and make important ethical decisions," she added.

In fact, a coder can be prosecuted if he or she has direct knowledge of an error occurring or facilitates mistakes, said Harman. This applies to a pattern, not isolated human error, she noted. "Everybody makes mistakes," she added. "But if you repeatedly make errors, you could put both yourself and your organization at risk."

Coders also should examine the entire medical record, rather than assigning the diagnosis codes for conditions on the face sheet or problem list without examining the entire record. "Don't do what's easier; go by quality," Harman said.

Coding professionals are expected to support the importance of accurate, complete and consistent coding practices, yet sometimes medical records are incomplete, presenting a challenge that coders cannot ignore, said Youmans. "If incomplete medical records are a pattern," she said, "it's a systems issue you need to address."

Coding professionals should maintain and continually enhance their coding skills, as they have a professional responsibility to stay abreast of changes in codes, coding guidelines, and regulations, said Harman, adding that it is not enough to take a coding course every few years. Coders need to stay up-to-date by taking more frequent courses and reading industry literature, she said. "It's a lifelong process," she said.

To improve communication of coding changes to medical staff, Harman suggested, physicians could educate coders about medical procedures, while coders could speak with physicians about the many variations of codes for each condition. Newsletters also can help improve communication, she said. "It doesn't take a lot of time to read [and] it gets the message across," she said.

Other ideas she presented include: purchasing current coding books for medical staff, identifying key coding staff to educate physicians on coding changes and documentation issues, and showcasing resolved coding and documentation issues with key staff and physicians and holding monthly meetings.

For more information on AHIMA's Code of Ethics (2004) visit: www.ahima.org. ■

CCH Washington Bureau, April 4, 2005

Antitrust

DOJ requires hospitals to terminate illegal market-allocation agreements

by Gene' Stephens, JD, Contributing Editor

Two community hospitals allegedly entered into market-allocation agreements for cancer and cardiac surgery services that allegedly would unreasonably restrict competition and consumer choice for those services in southern West Virginia according to the Department of Justice (DOJ). The agreements allegedly allocated markets and customers for cancer and cardiac surgery services between the two hospitals within a nine-county area. The agreements further allegedly restricted the ability of both hospitals to apply for, finance or participate in a Certificate of Need (CON) to provide cancer and cardiac surgery services with any other provider outside of the agreement provisions. In addition, both agreements allegedly improperly placed restrictions on the offering and sharing of any new technologies or modalities for the diagnosis and treatment of cancer and cardiovascular disease to the detriment of patients and consumers.

In its complaint, the DOJ described the likely harmful effects that could result from the cancer and cardiac surgery agreements, which included: (1) a denial of the benefits of competitive pricing for managed-care purchasers, their enrollees and employees and patients in southern West Virginia; (2) a decrease in the quality of cancer and cardiac-surgery services as a result of the absence of competition between the two hospitals; (3) the loss of patient choice in selecting a hospital to provide cancer or cardiac surgery services in the southern West Virginia region; and (4) a demise in provider incentives to offer or innovate new cancer and cardiac surgery services.

The complaint filed by the DOJ on March 21, 2005, further describes the two hospitals as the only general acute-care hospitals in Mercer County, West Virginia. Both hospitals were head-to-head competitors in cancer services and potential competitors in cardiac-surgery services. The DOJ further explained that the Sherman Act clearly prohibits hospitals and other competitors from engaging in market allocation schemes. A competitive impact statement and proposed consent decree was simultaneously filed by the DOJ, along with its complaint, that would prevent the two hospitals from obtaining a CON relating to cancer or cardiac-surgery services. The competitive impact statement further prohibits the two hospitals from entering into agreements with other providers concerning cancer or cardiac-surgery services without the prior approval of the government. ■

Department of Justice Press Release, March 21, 2005, ¶610,056

Fraud and Abuse

OIG settles alleged pharmaceutical referral scheme for $5.975M

by Gene' Stephens, JD, Contributing Editor

An institutional pharmaceutical company agreed to pay $5.975 million to settle allegations that it received illegal pharmaceutical business referrals as part of the purchase of a small state pharmacy. The Office of Inspector General (OIG) entered into both settlement and corporate integrity agreements (CIA) with the pharmaceutical company for the company's alleged violations of the anti-kickback statute and civil monetary penalties laws. The OIG alleged that the pharmaceutical company paid an excessive amount for the purchase of a state pharmacy in return for a commitment of Medicaid and Medicare pharmacy referrals from the sellers for the next seven years. The pharmaceutical company also stood to receive resident referrals from the pharmacy seller's nursing and assisted living facilities, which served approximately 2,800 residents.

The terms of the five-year CIA provide for initial and annual training on the provisions and sanctions of the anti-kickback statute, as well as require the pharmaceutical company's compliance program officer to provide examples of prohibited arrangements as part of the training. The CIA further requires the pharmaceutical company to engage an independent review organization within 90 days after the effective date of the Agreement to ensure compliance with anti-kickback provisions and civil monetary penalty laws. In addition, the CIA requires that the pharmaceutical company create and maintain a database for certain transactions covered under the Agreement to ensure that existing and new arrangements do not violate the anti-kickback statute. The $5.975 million settlement is the largest paid in an OIG civil monetary penalty and anti-kickback case. ■

OIG Press Release, ¶420,099