CCH Health Care Compliance LETTER

Volume 11, Issue 18 health.cch.com September 2, 2008

Wolters Kluwer Law & Business

OIG allows medical center's plan

Although a medical center's arrangement to pay two physician practice groups a share of the first year cost savings directly attributable to changes made in the groups' practices constituted an improper payment to induce reduction or limitation of services under anti-kickback regulations, the Office of Inspector General (OIG) would not seek sanctions against the medical center because the plan included sufficient safeguards to reduce the risk of increased referrals. The hospital agreed to pay the orthopedic and neurosurgery groups 50 percent of the savings achieved, which would be distributed to the group's members on a per capita basis in the prohibited remuneration agreement.

These arrangements are designed to align incentives by offering physicians a portion of a hospital's cost savings in exchange for implementing cost saving strategies. To develop the arrangement, the medical center conducted a study of historic practices in the surgical groups and identified 36 areas in which costs could be saved. In general, the medical center recommended (1) "use of biologicals" as needed, and (2) product standardizations of devices and supplies. Safeguards were set up to protect against inappropriate reductions in services.

Anti-kickback. The OIG would not seek sanctions under the federal anti-kickback statute because the arrangement: (1) had safeguards that reduced the likelihood that it would be used to attract referring physicians or increase referrals from existing physicians; (2) was structured to eliminate the risk that it would be used to reward other physicians who referred patients to the two practice groups; and (3) set out with specificity the particular actions that generated the cost savings on which payments were based.

Monetary penalties. The OIG would not impose civil monetary penalties against the hospital because: (1) the specific cost saving actions and resulting savings were clearly and separately identified; (2) the medical center and practice groups proffered credible medical support that the implementation of the recommendations do not adversely affect patient care; (3) the amount paid under the arrangement was calculated based on all services regardless of the patients' insurance coverage, subject to the cap on payment for federal health care program procedures; (4) the arrangement protected against reductions in services by utilizing objective historical and clinical measures to establish baseline thresholds beyond which no savings accrue to the two practice groups; (5) the practice groups had available the same selection of devices and supplies after implementation of the arrangement as before; (6) the medical center and practice groups provided written disclosures of their involvement in the arrangement to patients whose care may have been affected; (7) the financial incentives were reasonably limited in duration and amount; and (8) any incentive for an individual surgeon to generate disproportionate cost savings was mitigated because the group distributed profits on a per capita basis. ■

OIG Advisory Opinion, No. 08-09B, Aug. 7, 2008, ¶500,188.

Experts identify challenges associated with EHR systems

Electronic health records (EHR) systems must be supported by specific functionality to properly maintain business records in the support of regulatory, payment, and litigation compliance, according to Michelle Dougherty and Rita A. Scichilone, of the American Health Information Management Association.

Dougherty and Scichilone, provided advice to compliance officers and professionals on critical issues that need to be addressed for a "compliant EHR" system at a seminar sponsored by the Health Care Compliance Association.

Compliant EHR systems. Compliance professionals play an important role in the EHR system selection process. The burden is on the purchaser and the user of these tools to assure that in actual use the EHR system chosen qualifies as a legal record. Regardless of the format – paper, hybrid, or fully electronic – a record must meet the requirements of the official legal record for the organization.

Health care entities and vendors sometimes neglect to build in the record management processes and system capabilities needed to ensure the electronic rather than the paper version can stand as the legal business record. Information in an EHR system that does not qualify as a medical record, becomes hearsay, not a bona fide record, and its integrity for any and all uses becomes suspect. This "legal EHR" is a subset of content within the EHR system.

Both manual and electronic medical record systems should:

- maintain a medical record for each patient;
- properly file and retain each record to ensure prompt retrieval; and
- be accessible to authorized users, and protected from loss, destruction, alteration, reproduction, or theft.

Risks and concerns. Not addressing legal and compliance needs may result in:

- challenges to documentation that supports billing;
- potential increase in litigation costs; and
- potentially higher settlements.

Compliance professionals must be aware of gaps in the maintenance of these legal EHR systems, especially in metadata. Limited, inaccessible metadata tools result in event logs that may not be available at reasonable cost or at all. Records potentially may be overwritten because of missing data elements essential for proper record keeping.

There are four areas of concern for a compliant EHR: (1) authorship integrity, (2) auditing integrity, (3) documentation integrity, and (4) patient identification and demographic accuracy.

To preserve authorship integrity, EHRs must allow for multiple authors or entries for the same record. Otherwise, in situations in which an EHR limits entries to a medical record by one author, claims may reflect the wrong provider or service resulting in improper reporting of services. Auto-authentication, whereby the system or mechanism in place approves or updates entries without user review or input, results in perception of fraud because the documentation may support payments for services rendered by an individual not authorized to perform said services.

Additionally, the ability to detect when an entry was created, borrowed, modified or deleted is necessary to maintain the integrity of audits of EHR systems. This auditing functionality must always be on to prevent inappropriate alterations in the record.

In addition, an EHR system that relies upon documentation templates to save time may result in incorrect information or codes entered, not reflective of actual clinical service. Finally, in the purview of patient identification, automated or default entries, can result in fraudulent charges if registration status or place of service is misrepresented. Patient safety and care quality issues would be impacted.

Conclusion. Compliance officers must be included in the discussion when new EHR applications are evaluated. In addition, end users must effectively communicate with vendors to ensure that legal and compliance requirements are addressed in EHR systems' functionality.

CCH Chicago Bureau, Aug. 12, 2008.

CCH Health Care Compliance Letter

Portfolio Managing Editor
Pamela K. Carron, J.D., LL.M

Coordinating Editors
Susan Smith, J.D., M.A.
Harold Bishop, J.D.
Anthony Nguyen, J.D.
Amber Bollman, J.D.

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

Designer
Laila Gaidulis

Requests for information about article submission and comments from readers are welcome and should be directed to Susan Smith at susan.smith@wolterskluwer.com, Tel. 847-267-2780, 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, a Wolters Kluwer business, 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.

ADA, RA mandate effective communication for hearing-impaired

A hospital's failure to provide a sign language interpreter for a hearing impaired patient when she was hospitalized with a life-threatening condition raised a genuine issue of material fact as to whether the hospital violated the Americans with Disabilities Act (ADA) and the Rehabilitation Act (RA), according to the U.S. District Court for the Middle District of Georgia.

A genuine issue of material fact also existed regarding the patient's claim for compensatory damages based upon infliction of emotional distress, but did not exist with respect to punitive damages based upon willful misconduct, because punitive damages may not be awarded in private suits brought under §202 of the ADA and §504 of the RA.

Communication provided by the hospital. The court said that the ADA supporting regulations charged the hospital with the responsibility of effectively communicating with the patient as it would with hearing patients and that the hospital had a responsibility to furnish the patient with a qualified interpreter if the patient wanted one.

The hospital argued that relying upon

(1) written messages to and from the patient;
(2) the patient's ability to read lips;
(3) a nonqualified interpreter friend; and
(4) her children as sign language interpreters

were all effective means of communicating with her doctors and hospital staff.

The hospital contended that the patient had effective means of communication because she was able to consent to every surgical and diagnostic procedure that she underwent at the hospital. According to the hospital, because the patient was able to communicate through all these different methods, it was not put on notice that the patient needed additional auxiliary aids to communicate with hospital staff. In addition, the hospital pointed out that the ADA supporting regulations' use of the "where necessary" language supported its argument that auxiliary aids were not necessary for the patient to communicate with her doctors and to consent to medical procedures.

Patient's allegations. The patient argued that the hospital knew that she had requested an auxiliary aid in the form of a certified sign language interpreter and that communication methods relied on by the hospital were not the effective means outlined in the ADA's regulations.

She alleged that her friend's interpretive skills were not sufficient to meet her needs, and that she had requested a qualified interpreter, but was not given one until a month after she was hospitalized.

The patient also alleged that having a tube forced down her throat was intentional infliction of emotional distress because she did not have an interpreter to explain the procedure to her before it was performed.

Court's opinion. The court concluded that ["it] cannot be said that, as a matter of law, [that the] hospital complied with the federal regulations charging it to provide effective communication to" the patient while she was at the hospital. The patient's allegations, if true, meant that the hospital had not complied with the federal regulations created to effectuate the ADA, the court said. The regulations requiring effective means of communication for the patient would not be "satisfied by relying on interpretation performed by [the patient's] children where they were not available to be present at every interaction with [the patient's] doctors and nurses."

The court also found that there was an issue of material fact as to whether the hospital exhibited bad faith by failing to secure a qualified interpreter for the patient. Finally, the court concluded that a fact finder would have to determine whether forcing a tube down the patient's throat qualified as intentional infliction of emotional distress. ■

Boyer v. Tift County Hospital Authority, U.S. District Court, Middle District of Georgia, July 31, 2008, Health Care Compliance Reporter, ¶800,547.

On The Front Lines

Understanding compliance legal standards in the HIPAA Security Rule, Part II

by John E. Steiner Jr., Esq., Health Care Compliance Advisory Board Member and Brittany Eberle

Part I of this article focused on legal standards required by the Security Rule. Part II will focus on enforcement and sanctions. It is important to recognize that CMS has discretion in applying sanctions. Approximately fourteen percent of cases opened by CMS have been closed by corrective action plans according to enforcement statistics released as of the end of June 2008.[26]

Many Security Rule violation complaints come to the attention of CMS through Privacy Rule complaints to the Office for Civil Rights (OCR). In turn, the OCR forwards Security Rule related complaints to CMS - specifically to the Office of E-Health Standards and Services (OESS). OESS initiates an investigation.[27] CMS has indicated that fines or sanctions may be levied for violations that are confirmed by its audits.[28]

Security Rule Enforcement and Sanctions

A covered entity faces sanctions if it violates or "fail[s] to comply" with the Security Rule.[29] CMS, however, has indicated a preference for seeking voluntary compliance before initiating its sanctioning process.[30] For instance, in some cases, CMS may be satisfied with a corrective action plan and may close the investigation without seeking monetary penalties.[31] Prompt response to a CMS request may also factor into CMS' consideration of an entity's compliance.[32]

As demonstrated by the recent events with Providence Health & Services, CMS may choose to resolve possible Security Rule violations with a resolution agreement. Though the agreement requires Providence to pay $100,000, CMS does not view this as a use of its ability to impose formal civil penalties.[33] In addition to the settlement agreement, the Providence resolution agreement includes a detailed corrective action plan. Under the plan, for the next three years, Providence must: (1) have HHS review and approve its policies and procedures, (2) provide to HHS evidence of implementation of its policies and procedures, (3) provide evidence of training of personnel on those policies and procedures, and (4) submit compliance reports to HHS. Additionally, Providence must conduct audits to confirm workforce compliance and assess additional vulnerabilities to Providence's ePHI. HHS also reserves its right, in the resolution agreement, to impose civil penalties if Providence breaches the terms of the agreement.[34]

CMS may impose sanctions for civil violations that carry monetary penalties. Whether a violation will result in fines turns on whether a covered entity can raise an affirmative defense that the violation was due to "reasonable cause" rather than "willful neglect." Willful neglect is a "conscious, intentional failure or reckless indifference to the obligation to comply" with a provision of the Security Rule. A reasonable cause defense is one that asserts that the circumstances were such that it "would make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the [HIPAA] provision violated."[35] A reasonable cause defense also must demonstrate that the violation was corrected within thirty days of when the covered entity knew, or should have known, of the violation's existence.[36]

"A person who knowingly...uses, or causes to be used, a unique health identifier, obtains [PHI], or discloses [PHI] to another person," including ePHI, can face criminal sanctions.[37] Criminal violations of HIPAA are handled by the Department of Justice (DOJ). The DOJ reviewed HIPAA and supplied guidance on the meaning of the words "person" and "knowingly." According to the DOJ, "person" refers to the covered entity and can include "directors, officers and employees," and "knowingly" requires "knowledge of the facts."[38] The maximum prison terms and fines increase if the use, acquisition, or disclosure of a unique health identifier or PHI was "committed under false pretenses," and increase further if the offense is "committed with intent to sell, transfer or use [PHI]."[39]

Security Rule Audits

Beginning with Piedmont Hospital in Atlanta, Georgia, the HHS Office of Inspector General (OIG) initiated the first series of government audits in 2007 to evaluate hospitals' compliance with the Security Rule.[40]

Shortly thereafter, CMS announced it would initiate audits for compliance with the Security Rule.[41] Although

the OIG and CMS audits seek similar information from audited covered entities, the scope of the audits is not the same. CMS' audits focus on Security Rule compliance and enforcement and primarily involve covered entities with previous HIPAA security complaints. In addition, CMS may audit entities with a high volume of records that may be more vulnerable to security breaches. On the other hand, OIG audits focus on CMS' oversight of the Security Rule at selected hospitals.[42]

At least one hospital audited by the OIG had the highest Medicare reimbursement in its region. Therefore, hospitals with high Medicare populations may be at greater risk of an OIG audit.

The information sought by these two government agencies is similar. Both track the standards and implementation specifications of the Security Rule and include addressable implementation specifications. CMS provides a sample interview and document request checklist as guidance for covered entities. A list of information reportedly requested by the OIG in the Piedmont audit has been unofficially released.[43] These two lists should be used for audit preparation and as guidance to assess HIPAA compliance by a covered entity.

"Keeping security issues in the forefront of a covered entity's compliance program is necessary in a world that is increasingly adopting electronic means of communication and recordkeeping."

Documentation

A crucial element for demonstrating compliance is documentation, which typically is a significant part of the HIPAA Security audit. The auditor will request documentation that the covered entity has conducted a risk analysis and developed security measures, including policies and procedures that respond to any identified vulnerabilities. As required under Providence's resolution agreement, auditors also will request documentation to demonstrate that policies and procedures have been implemented by the covered entity.[44]

Interviews with Key Personnel

Auditors will interview key members of a covered entity's Security Rule compliance team. Industry sources confirm that Security Rule audits will require significant involvement of the security officer. CMS' interview checklist also includes members of senior management, some of whom have significant roles in the implementation of various parts of the Security Rule, such as the president, chief executive officer, or director of the covered entity.[45] This portion of an audit is rooted not only in audit practices, but the requirements of the Security Rule. As noted earlier, the fourth general requirement mandates training of the workforce, and the standard for "Security Awareness and Training" specifically includes management on the list of workforce members who should be knowledgeable about Security Rule policies.[46]

Specific Areas of Audit Preparation

Industry sources have indicated that the OIG is interested in security vulnerabilities, access controls, and transmission security. The interest in security vulnerabilities is likely a by-product of auditing the risk analyses and risk management performed by the covered entity. In short, OIG may be trying to determine whether the covered entity has correctly assessed and appropriately responded to system vulnerabilities.

Access controls and transmission security are standards in the Security Rule. Both are technical safeguards. Access controls are designed to limit access to systems that contain ePHI.[47] Transmission security generally addresses the ability of unauthorized people or programs to access ePHI.[48] The standard, however, is specifically concerned with access that may occur during the transmission process.[49] CMS has indicated that both standards should be considered when covered entities allow remote access to their ePHI.

Remote Access to ePHI

Several sources indicate that remote access will be an audit priority. Changes in technology have increased the ability of healthcare providers and others to access and use ePHI remotely, either by devices or external systems. Though not expressly covered in the Security Rule, CMS released additional guidance that focuses on risks associated with remote use and access of ePHI. These risks include contamination of data due to viruses, loss or theft of portable devices, and inappropriate offsite access of ePHI by employees. The guidance describes security measures that may be reasonable and appropriate for covered entities to adopt when choosing to allow remote access. Those measures are more specific than the standards or implementation specifications in the Security Rule.[50]

Further deployment of e-health remote access is an important component of contemporary delivery of health care. Thus, new technologies may require implementation of new policies and procedures to meet the Security Rule's first four general requirements discussed earlier.

Conclusion

Keeping security issues in the forefront of a covered entity's compliance program is necessary in a world that is increasingly adopting electronic means of communication and recordkeeping. Government audits are a predictable reminder of this compliance priority. The information sought in these audits reinforces the importance of proactive programs. Government audits target existing risk assessments and implementation of security measures to address weaknesses in a covered entity's protection of ePHI. A workforce that is well informed of the policies and procedures that a covered entity has developed in response to its risk analysis and other standards will bolster a covered entity's position that it is not willfully neglecting its obligation to comply with the Security Rule. In addition, a well educated and trained workforce will likely decrease the number and severity of security incidents that may occur.

The Security Rule does not require a compliance program to prevent all security incidents. How a covered entity responds to a security incident it discovers or that is brought to its attention in the course of an OESS investigation or government audit should bear on a determination of liability. Using the compliance legal standards found in the Security Rule and in the CMS and OIG audit guidance may avert assessment of costly fines and public relations problems that may result from Security Rule noncompliance.

John E. Steiner Jr., Esq., CHC is the Chief Compliance Officer for UK Health Care of the University of Kentucky of Lexington, Kentucky. He previously served as Chief Compliance Officer and Privacy Officer for the Cleveland Clinic, as Senior Counsel for the American Hospital Association, and as a member of the health law department of a national law firm. He is a member of the CCH Health Care Compliance Editorial Advisory Board.

Brittany Eberle is a third year law student at the University of Kentucky. She is expected to graduate in May 2009.

[26] CMS, *CMS Enforcement Statistics Report: Open and Closed Cases by Type as of June 30, 2008,* 1 (2008), *available at* http://www.cms.hhs.gov/Enforcement/Downloads/EnforcementData0608.pdf.

[27] See Tony Trenkle, Key Note Address at the CMS & National Institute for Standards and Technology (NIST) Workshop, *HIPAA Security Overview*, 3, 8-9, Jan. 16, 2008, *available at* http://csrc.nist.gov/news_events/HIPAA-Jan2008_workshop/presentations/KeyNoteAddressCMS.pdf; Notice, 70 FR 15330, March 25, 2005. Audits are only a recent addition to the enforcement of the Security Rule. OIG, *CMS Security Audits Are 'Level Two of Compliance,' Experts Say; Risk Analysis and Preparation Advisable*, Vol. 70 No. 1, Guide to Medical Privacy & HIPAA Newsletter 6, February 2008.

[28] Nancy Ferris, *CMS to check hospitals for HIPAA security compliance*, Government Health IT, Jan. 17, 2008, *available at* http://www.govhealthit.com/online/news/350176-1.html.

[29] 45 C.F.R. §§ 160.302, 160.402.

[30] See Notice, *supra* note 27, at 15330-31.

[31] See Tony Trenkle, *supra* note 27, at 8; see *also* CMS, *CMS Enforcement Statistics Report: Open and Closed Cases by Type as of June 30, 2008*, 1 (2008), *available at* http://www.cms.hhs.gov/Enforcement/Downloads/EnforcementData0608.pdf.

[32] See Notice, *supra* note 27, at 15331; HHS *supra* note 4. Examples of enforcement for the Security Rule are *available at* http://www.cms.hhs.gov/Enforcement/03_HIPAA%20Case%20Examples.asp#TopOfPage.

[33] See Notice, supra note 27 at 15331; HHS supra note 4. Examples of enforcement for the Security Rule are *available at* http://www.cms.hhs.gov/Enforcement/03_HIPAA%20Case%20Examples.asp#TopOfPage.

[34] HHS & Providence Health Services, *Resolution Agreement*, 2, Appendix A, July 9 2008, *available at* http://www.hhs.gov/ocr/privacy/enforcement/agreement.pdf.

[35] Social Security Act §1176(a), (b)(3)(A)(i); 45 C.F.R. §§ 160,402, 160.410(a),(b)(3)(i).

[36] Social Security Act §1176(b)(3)(A)(ii); 45 C.F.R § 160.410(b)(3)(ii).

[37] Social Security Act §1177(a).

[38] DOJ, *Memorandum Opinion for The General Counsel Department of Health and Human Services and the Senior Counsel to the Deputy Attorney General on the Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6*, June 1, 2005, *available at* http://www.usdoj.gov/olc/hipaa_final.htm.

[39] Social Security Act §1177(b).

[40] OIG, *CMS Security Audits Are 'Level Two of Compliance,' Experts Say; Risk Analysis and Preparation Advisable*, supra note 27; Bob Brown, *Do Reports of a Recent Surprise Audit Indicate the Beginning of a New Security Rule Compliance Initiative?*, Vol. 9, No. 6 Journal of Health Care Compliance, 33 (November-December, 2007); CMS Launches HIPAA Security Compliance Audits, Vol. 11 No. 2 Employer's Guide to HIPAA Newsletter 3 (March 2008).

[41] See Nancy Ferris, supra note 28; *CMS Launches HIPAA Security Compliance Audits*, supra note 40.

[42] Tony Trenkle, *supra* note 27, at 12; *CMS Launches HIPAA Security Compliance Audits*, *supra* note 40; Ferris *supra* note 28.

[43] See CMS, *Sample – Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews* (2008) *available at* http://www.cms.hhs.gov/Enforcement/Downloads/InformationRequestforComplianceReviews.pdf; Bob Brown, *supra* note 40, at 33 (containing the list of items requested of Piedmont Hospital by the OIG).

[44] See CMS, *Sample – Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews*, *supra* note 43; Bob Brown, *supra* note 40, at 33; Nancy Ferris, *supra* note 28. OIG, CMS *Security Audits Are 'Level Two of Compliance,' Experts Say; Risk Analysis and Preparation Advisable*, *supra* note 27.

[45] See *also* CMS, *Sample – Interview and Document Request for HIPAA Security Onsite Investigations and Compliance Reviews*, *supra* note 43.

[46] 45 C.F.R. §§ 164.306(a)(4), 164.308(a)(5)(i).

[47] 45 C.F.R. § 164.312(a)(1). Specifically, this standard seeks to limit access to programs and people that have been previously determined to need access. Id. Covered entities should determine who has access based on the information access management standard. 45 C.F.R. § 164.308(a)(4).

[48] 45 C.F.R. § 164.312(e)(1).

[49] CMS, *Security Guidance for Remote Access*, 4,6 (2006), *available at* http://www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806.pdf.

[50] *Id.* at 1, 4-6.

Medicaid

Experts urge providers to plan ahead for MIP audits

As the Medicaid Integrity Program (MIP) enters the implementation stage, providers should prepare for more intensive review by a new group of auditors, the Medicare Integrity Program contractors (MICs), according to James G. Sheehan, New York's Medicaid Inspector General. Sheehan and Brian Flood, managing director of KPMG, advised compliance officers to strengthen their compliance programs during a Health Care Compliance Association Seminar.

MIP focus. The MIP focuses on quality of care, patient outcomes and failure to meet professional standards. The program requires adverse event reports and data mining to identify patterns of poor outcomes, fraud or abuse. In addition, CMS has directed state Medicaid programs to deny payment for costs resulting from " never events" as Medicare is doing. Under the program, physicians or providers involved in multiple never events will be identified and investigated.

Contractors' role. MIP contractors (MICs) will be assigned either to surveillance or audits of particular providers. The surveillance group uses data mining and other techniques to identify practitioners or providers who should be audited. Data mining can reveal unrecognized causes of poor outcomes or increased costs. For example, of the millions of central venous catheters inserted each year, one in 20 is associated with a bloodstream infection resulting in 250,000 preventable bloodstream infections per year. In addition to the burdens on patients and families, these preventable infections add an average of $25,000 to the cost of a hospital stay ($45,000 for intensive care unit stays).

The audit group will examine policies, procedures, and prevention more closely than before. For example, with respect to utilization review, the auditors will look for a provider's response to reported events and the actions it had taken to prevent future occurrences. They will analyze the lines of communication between staff at various levels, including the compliance officer and the governing body, and will look for adverse events that may not have been reviewed by the appropriate committee or were not reported as required.

MICs v. RACs. In contrast to the recovery audit contractor (RAC) program that began last year, the MICs: (1) are not bound by deadlines; (2) are not limited to the three preceding years; and (3) may investigate or audit despite the previous involvement of a state agency or another contractor.

Role of the governing body. New York was the first state to adopt a mandatory compliance program for Medicaid providers. It broadened the reach of compliance requirements by focusing on quality of care, return on investment, and prevention of identified risks. In addition to written policies and a code of conduct, the state emphasized the responsibility of an organization's governing body for compliance issues. The identified compliance officer must report directly to the governing body, and all new board members must undergo training. Under New York's guidelines, failure to report a violation may result in discipline.

MIP also will focus on the involvement of the governing body of a provider to determine whether: (1) the body is aware of quality issues generally; (2) identified quality issues are addressed; and (3) best practices are adopted. ■

CCH Chicago Bureau, Aug. 14, 2008.

Medicare

$16.7 million in performance pay earned by physician groups

During the second year of the Physician Group Practice (PGP) Demonstration all 10 participating physician groups achieved benchmark or target performance on at least 25 out of 27 quality markers for patients with diabetes, coronary artery disease, and congestive heart failure, according to CMS. As a result, the 10 groups earned $16.7 million in incentive payments for improving health outcomes and coordinating the overall health care needs of assigned Medicare patients. Five of the physician groups achieved benchmark quality performance on all 27 quality measures. The PGP Demonstration is one of CMS' value-based purchasing initiatives, designed to tie Medicare payments to cost and quality measures.

PQRI incentives. The 10 physician groups participating in the PGP Demonstration agreed to place their related Physician Quality Reporting Initiative (PQRI) incentive payments at risk for performance on the 27 quality measures reported under the demonstration. All physician groups received at least 96 percent of their PQRI incentive payments, with five groups earning 100 percent of their incentive payments. A total of $2.9 million in PQRI incentive payments was paid out to the 10 groups under the demonstration.

Quality of care improvement. The groups also improved the quality of care delivered, increasing their quality scores an average of nine percentage points across the diabetes mellitus measures, 11 percentage points across the heart failure measures, and five percentage points across the coronary artery disease measures. These groups achieved their levels of performance by: (1) having "clinical champions" (physicians or nurses who are in charge of quality reporting for the practice), (2) redesigning clinical care processes, and (3) investing in health information technology. The investment in electronic health records and patient registries allowed practices to more easily identify gaps in care, alert physicians to these gaps, and provide interim feedback on performance.

Favorable financial performance. In addition to achieving benchmark performance for quality, several physician groups also experienced favorable financial performance under the pay for performance methodology. The four physician groups earned $13.8 million in performance payments for improving the quality and cost efficiency of care as their share of a total of $17.4 million in Medicare savings.

CMS Medicare News, Aug. 14, 2008. ■

continued on page 8

Medicare (cont.)

HHS announces transition to ICD-10 code sets

New code sets that would improve disease tracking and speed up the development of an electronic health care environment could take effect by October 2011. HHS has announced a proposed regulation that would update the code sets used to classify and report health care diagnoses and inpatient hospital procedures. The regulation would replace the ICD-9-CM (International Classification of Diseases, Ninth Revision, Clinical Modification) code sets, which were adopted in 2000, with ICD-10 (Tenth Revision) code sets.

HHS officials say the long-anticipated transition to new code sets will improve the quality of electronic health records (EHR) by providing greater detail. While the outdated ICD-9, which was published by the World Health Organization in 1977, contains only 17,000 codes and is expected to start running out of available codes next year, ICD-10 can accommodate more than 155,000 codes. Officials say the availability of new diagnostic codes will allow health care providers to identify conditions more precisely in EHRs and assign new codes to contemporary disease outbreaks.

The need to update the coding system has been championed by the health information management industry for several years. ICD-9 does not meet current health care data needs and cannot support the transition to interoperable health data exchange in the U.S., the American Health Information Management Association said in a July 2007 statement urging HHS to adopt the ICD-10 code set immediately. "Simply put, we're trying to describe early 21st century with mid-1970s classification."

Although transition to ICD-10 will require some upfront expenditure, HHS officials say each year of delay would create additional costs, as information systems and software would have to be converted retroactively. Public comments on the proposed rule will be accepted until October 21. The regulation would become effective October 1, 2011. ■

CMS Press Release, Aug. 15, 2008; AHIMA Statement, July 2007.

In the News

Hospital Compare consumer Web site enhanced

CMS' *Hospital Compare* consumer Web site now includes: (1) a 30-day mortality measure for pneumonia, and (2) publicly reported measures for asthma care of children. The pneumonia mortality outcome measures are risk-adjusted and take into account previous health problems to "level the playing field" among hospitals. The measures are intended to help ensure accuracy in performance reporting. The children's asthma care measures include relievers for inpatient asthma and systemic corticosteroids for inpatient asthma, and mark the first time *Hospital Compare* has provided quality information on children. CMS has released information that will allow consumers and hospitals to drill down beyond the categorical information of the mortality measures to determine whether the hospital's mortality rate is "Better than," "No different from," or "Worse than" the U.S. national rate. This new data information includes each hospital's risk-standardized mortality rate, an estimate of the rate's certainty, and the number of eligible cases for each hospital. To help hospitals use the 30-day mortality data as a quality improvement tool, CMS has provided detailed reports to each hospital listed on the Web site (http://www.hospitalcompare.hhs.gov/).

CMS News Release, Aug. 20, 2008.

New code applies to claims denied for Stark law violations

Beginning January 5, 2009, Medicare contractors that deny claims because of noncompliance with physician self-referral prohibition legislation will make the reason for those denials explicitly known to health care providers. CMS has added a new Claim Adjustment Reason Code (CARC #213) that contractors will use when denying claims on the basis of Stark law violations. Stark outlaws physicians from referring Medicare patients for certain designated health services to any entity with which the physician has a financial relationship. A "financial relationship" includes ownership or investment interests and compensation arrangements. A referral to an entity with which a physician's immediate family member has a financial relationship now is also prohibited by Stark. Until now, there was no specific code to indicate to health care providers that their claims were denied because of noncompliance with the physician self-referral prohibition.

Medicare Claims Processing Manual, Pub 100-04, Transmittal 1578, Aug. 15, 2008.

Practitioners create website to help with Form 990

The 990 Coalition for Hospitals has designed a web site to help nonprofit hospitals and their advisors with Internal Revenue Service (IRS) Form 990, Return of Organizations Exempt From Income Tax. The mission of the coalition is to promote accurate and standardized reporting of community benefit and related information on the revised Form 990 and Schedule H. Participants in the coalition are the American Health Lawyers Association, Catholic Health Association, the Healthcare Financial Management Association, and VHA, Inc. The Web site provides: (1) a central source for current information on IRS activity and instructions; (2) a forum for hospitals and their advisors to share information on planning and implementation efforts for filing Form 990 and Schedule H; (3) guidelines for completing Form 990 and Schedule H; (4) annotation of Schedule H with expert advice; (5) coalition sponsored audio conferences; and (8) a calendar of events of educational programs regarding Form 990. The Internet address is: www.990forhospitals.org.

CCH Exempt Organizations Reports, No. 409, Aug. 15, 2008.