### Columns

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>From the Editor—Roy Snell</td>
<td>Finding and Fixing Problems Is What We Are Supposed to Do</td>
</tr>
<tr>
<td>33</td>
<td>Electronic Resources—Catherine M. Boerner</td>
<td>e-Health and Quality of Care: Two Areas Every Compliance Officer Should Know About</td>
</tr>
<tr>
<td>35</td>
<td>HIPAA—Bob Brown</td>
<td>The Number of Online Personal Health Records Is Growing, but Is the Data in These Records Adequately Protected?</td>
</tr>
<tr>
<td>37</td>
<td>Best Practice—Julene Brown</td>
<td>Compliance Teams – Are They a Good Thing?</td>
</tr>
<tr>
<td>41</td>
<td>QIO—Harry M. Feder</td>
<td>CMS and QIOs Encourage Physician Use of EHRs</td>
</tr>
<tr>
<td>43</td>
<td>Compliance Officer—Alice G. Gosfield</td>
<td>Doing What Really Matters: The Compliance Connection to Health Care Quality</td>
</tr>
<tr>
<td>45</td>
<td>Auditing and Monitoring—Georgette Gustin/Lori Cannady</td>
<td>You May Want to Revist (and Reevaluate) Your Annual Risk Work Plan</td>
</tr>
<tr>
<td>47</td>
<td>Health Information Management—Beth Hjort</td>
<td>AHIMA Report Addresses Evolving Role of Health Care Privacy and Security Officers</td>
</tr>
<tr>
<td>49</td>
<td>Hot Line—Richard Kusserow</td>
<td>Should Your Hot Line Be Outsourced, or Should it Be Operated in House?</td>
</tr>
<tr>
<td>51</td>
<td>Settlements—Scott A. Memmott/Rebecca C. Fayed</td>
<td>DOJ Issues Revised Principles for Prosecuting Corporate Fraud</td>
</tr>
</tbody>
</table>

### Features

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Corporate Culture—Frank Sheeder</td>
<td>Excuse You for Bumping into Me!</td>
</tr>
<tr>
<td>55</td>
<td>National Provider Identifier—Jennifer Harris Smith</td>
<td>Update on NPI Implementation: CMS Contingency Plans</td>
</tr>
<tr>
<td>57</td>
<td>Coding and Billing—Melinda S. Stegman</td>
<td>Physician Services “Place of Service” Reporting: Why All Providers Should Be Concerned</td>
</tr>
<tr>
<td>61</td>
<td>Lab—Christopher Young</td>
<td>Compliance Professionals Often Have to Focus Their Resources on Areas That Pose the Greatest Risk</td>
</tr>
</tbody>
</table>

### For the Record

<table>
<thead>
<tr>
<th>Page</th>
<th>Title</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>31</td>
<td>Roy Snell</td>
<td>Kimberly Brandt Discusses the Program Effectiveness Project, Medicare and Medicaid Risk Areas, and Helpful Resources</td>
</tr>
</tbody>
</table>

---

**Volume 9, Number 3 May–June 2007**
This magazine is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting or other professional service and that the authors are not offering such advice in this publication. If legal advice or other expert assistance is required, the services of a competent professional person should be sought. All views expressed in the articles and columns are those of the author and not necessarily those of CCH, a Wolters Kluwer business, or any other person.

Phonocopying or reproducing in any form in whole or in part is a violation of federal copyright law and is strictly forbidden without the publisher's consent. No claim is made to original governmental works; however, within this product or publication, the following are subject to CCH's copyright: (1) the gathering, compilation and arrangement of such government materials; (2) the magnetic translation and digital conversion of data, if applicable; (3) the historical, statutory and other notes and references; and (4) the commentary and other materials.

Editorial Board

CHRIS ANDERSON
Vice President and Chief Compliance Officer
Triad Hospitals, Inc.
Plano, TX

JOE BECK
Vice President
Business Ethics and Compliance
Quorum Health Resources, LLC
Brentwood, TN

CATHERINE M. BOERNER, J.D.
President
Boerner Consulting, LLC
Milwaukee, WI

RICHARD P. KUSSEROW
President
National Hotline Services, Inc.
Fredericksburg, VA

VICKIE L. MCCORMICK
Chief Compliance Officer
St. Jude Medical, Inc.
St. Paul, MN

FRANK SHEEDER
Partner
Jones Day
Dallas, TX

DION P. SHEIDY, CPA
Partner
PricewaterhouseCoopers, LLP
Pittsburgh, PA

THOMAS H. SUDDATH JR., ESQ.
Attorney
Montgomery, McCracken, Walker & Rhoads, LLP
Philadelphia, PA

DEBBIE TROKLUS, CHC
Assistant Vice President
Health Affairs/Compliance/HIPAA
University of Louisville
School of Medicine
Louisville, KY

SHERYL VACCA
Director
West Coast Compliance Practice
Deloitte & Touche
Sacramento, CA

L. STEPHAN VINCZE, J.D.
President and CEO
Vincze & Frazer, LLC
Atlanta, GA

ALAN YUSPEH
Senior Vice President
Ethics Compliance & Corporate Responsibility
HCA
Nashville, TN

© 2007 CCH. All Rights Reserved. This material may not be used, published, broadcast, rewritten, copied, redistributed, or used to create any derivative works without prior written permission from the publisher.

Journal of Health Care Compliance (ISSN: 15208) is published bimonthly by CCH.

Postmaster: Send address changes to Journal of Health Care Compliance, 7201 McKinney Circle, Frederick, MD 21704.

Subscription Price: $259 per year plus postage, handling and appropriate state sales tax. Simple issue price: $52.

Business and circulation: Distribution Center, Aspen Publishers, 7201 McKinney Circle, Frederick, MCD 21704.

Permission requests: For information on how to obtain permission to reproduce content, please go to the Aspen Publishers website at www.aspenpublishers.com/permissions.

Purchasing reprints: For customized article reprints, please contact FostReprints at 866-879-9144 or go to FostReprints website at www.fostereprints.com.
Finding and Fixing Problems Is What We Are Supposed to Do

Despite the Distractions that May Occur, It Is Important Not to Lose Focus

I am amazed at how many things we can find to do other than find and fix problems. It concerns me because finding and fixing problems is what compliance is ultimately all about. The reason our profession exists is because those who came before us could not fix the problems.

Many of the congressional hearings on corporate fraud have a litany of people explaining that they were aware of the problems but did not do anything about those problems. When asked, they say it wasn't their job. When asked, they say nobody listened. It is the compliance professional's job to find and fix problems even though it is hard.

We have a lot of distractions. We have distractions that caused those who came before us to be unsuccessful. We have distractions — yes, the same distractions that those before us faced — that can draw us away from finding and fixing problems. They are tempting distractions because they are not as painful as finding and fixing problems.

I know people who write constantly. They write policies and procedures. They write memos and plans. Sometimes I think people write to escape the painful chore of finding and fixing problems.

While Rome is burning, some people write. I know people who love to educate. They spend a significant amount of their time teaching and talking. Oddly enough I have met those who love to audit but cannot bring themselves to take the bad news to those affected. There are many distractions, and it's getting worse.

There are a lot of people not in the compliance profession trying to tell us how to do our job. They feel they know what we should be doing. There is always a lot of talk about exotic plans to analyze or study risk, but very few volunteer to go into a difficult situation to fix a problem.

There is now something called governance risk and compliance (GRC). It is a phrase developed by those who want to be where the action is, compliance. They feel they must make it more interesting or palatable to chief executive officers. We used to call these things the management program of the month, i.e., total quality management. Lots of talk, cool slides, a nice suit, but the suit is empty. I have heard a couple GRC presentations. We all sit there mesmerized by the complexity, and it all sounds very im-
portant. When the presentation is over, no one has a clue what the presenter said.

Compliance involves a focused use of the seven elements to find and fix problems. We must make sure that at the end of the day we find and fix problems. Our profession exists simply because those who came before us refused to do the dirty work. Everyone talked a good game, but when the going got tough, the talkers were nowhere to be found. Don’t lose focus. Make sure that all you do all day long is designed to find and fix problems.
Combining Disciplines: Making the Connection Between Compliance, Risk, and Quality Management

Recent Corporate Integrity Agreement Illustrates Heightened OIG Focus on Quality of Care

D. Scott Jones

Conventional Wisdom: Divide Quality, Compliance, and Risk

Health care organizations tend to segregate operations and related risks into management “silos.” The conventional wisdom is that segregation of risk allows large or complex organizations to address issues and tasks by breaking them down into manageable components. The division of tasks into segregated units of work also is a characteristic of large organizations with complex structures and strong departmental management.¹

As the prevailing regulatory and liability operating environment becomes increasingly complex in health care, the division and segregation of risk becomes in itself a risk exposure. Many health care organizations have not yet fully embraced the concept of developing connections between the disciplines of quality management, corporate compliance, and risk management. Likewise, organizations that provide malpractice and general liability insurance are well behind the curve when it comes to connecting the importance of risk management, regulatory compliance, and quality management as loss prevention tools.

Traditional segregated structures for these related functions are no longer the best protection for a health care organization in the current regulatory, medical liability, and enforcement climate. Complex changing risk environments will force evolution of the jobs traditionally performed by the compliance officer, risk manager, and quality manager. Organizations that recognize the importance of combining efforts will be much better prepared to deal with issues such as pay for performance,
quality and compliance investigations, and increased associated medical liability risk.

**The Quality Avalanche**

For years, the compliance profession has heard a quality of care message from Office of Inspector General (OIG), CMS, and Department of Justice (DOJ) leaders. Notable among these message bearers are the following: Lewis Morris, who was instrumental in the development of the OIG Long-Term Care Compliance Guidance; Kimberly Brandt, who was co-developer of the OIG Compliance Guidance for Physician Practices; and Patrick Meehan and Jim Sheehan, who are U.S. attorneys recognized as leading prosecutors of quality and compliance issues. Even as compliance began to function as a profession in health care, regulators and prosecutors addressed the need for quality improvement in the delivery of health services.2

In recent years these messages have become even more urgent, as studies from organizations such as the National Institutes of Health (NIH), the Institute of Medicine (IOM), and others addressed the injuries and deaths associated with medical errors and inadequate quality of care. In 2005, an article in the *Journal of the American Medical Association* (JAMA) cited studies in two states that illustrated that hospital progress toward developing patient-centered safety programs is proceeding at a slow pace. The journal noted:

> Data are consistent with reports that patient safety system progress is slow and is cause for great concern...."3

The latest public advertising and education campaign of the NIH notes that, according to the IOM, 120 patient deaths per day occur in U.S. hospitals due to medical errors — more than are due to motor vehicle accidents, breast cancer, or AIDS.4 A widespread perception of inadequate quality in health care services has been driven by these widely promoted studies, highly publicized legal and regulatory actions, and an aggressive plaintiff's bar that effectively and widely uses mass media.

In addition to increased demands for measurable quality improvements, most health care systems are struggling with staffing shortages and the sheer volume of patients that must be seen in order to meet demand or maintain economic viability. Patient volume increases are driven by an older population with more comorbidities and diagnostic needs; population growth surges in suburban areas; and the need to process larger numbers of patients more quickly in many medical services due to limited reimbursement.

Staffing concerns that lead to quality concerns are evident in current nursing staff shortages and a projected pending shortage of physicians. Current forecasts project physician shortfalls of 85,000 to 200,000 doctors by the year 2020 and project that patient demand for care at current rates will far outstrip the number of physicians who will be available in the United States by that time.5

Combined regulatory compliance and quality enforcement already has affected some areas of the health care industry, such as long-term care. A number of landmark cases, such as *U.S. v. Borne & Dynastar* (E.D. La. 2003-05), include findings that the facility and management systemically failed to provide adequate care for residents. The case included prosecution under 18 U.S.C. §1347, as a criminal scheme to defraud health care programs.

Hospital and physician cases prosecuted by the DOJ for failure to provide appropriate quality of care include the 2003 United Memorial Hospital case, which resulted in a deferred prosecution agreement for inadequate quality related to anesthesia and pain management services. Concerns included the volume of patients treated, a lack of sterile technique, a lack of improvement among patients, and patient complaints.

The Redding Hospital investigation in 2005 involved allegations of lack of medical
necessity involving cardiac surgeries. Prosecutors noted that 13 medical malpractice lawsuits were filed against involved physicians between 1988 and 2002. This Tenet Healthcare Corporation case was triggered by a quality of care whistleblower.

Many compliance officers and quality of care advocates clearly see a new regulatory approach toward including quality of care as a component of regulatory compliance programs. This is evident in many developing initiatives, such as private and public sector pay-for-performance (P4P) programs, Reporting Hospital Quality Data for Annual Payment Updates (RHQDAPU) under the Medicare Modernization Act of 2003, and hospital mandatory reporting requirements for serious events and incidents in 24 states.

Health care is experiencing a quiet avalanche of quality-oriented regulation that will directly affect the way care is delivered in every venue. A key indicator of this avalanche of quality measures is the profound emphasis on quality of care and compliance seen clearly in the latest corporate integrity agreement (CIA) issued for Tenet Healthcare Corporation.

**Tenet’s New CIA: Why It’s Different**

On September 27, 2006, Tenet Healthcare Corporation signed an annual update of its ongoing CIA with the OIG. While the new agreement has many similarities to other CIAs, it also is profoundly different.

For the first time, the OIG has inserted in this landmark CIA very specific language directed at quality of care measures and improvement. Language in the document and appendices specifically addresses quality improvement, quality indicators and measures, and physician-led quality monitoring. Twenty-three of the documents’ 63 pages address or name quality issues to some degree.

The impact of the new Tenet CIA is subtle and powerful. For the first time, specific groups of quality monitors and indicators are required by the OIG for a large, national organization of approximately 70 hospitals. To avoid further prosecution under the civil False Claims Act (FCA), Tenet has agreed to implement these measures as part of the CIA and its internal corporate compliance program.

The Tenet CIA includes requirements for measures such as:

- A clinical quality department, including a chief medical officer, senior officers, and clinical quality staff;
- Clinical audits;
- Physician credentialing;
- Physician privileging;
- Physician peer review;
- Evidence-based medicine programs;
- Standards of clinical excellence;
- Utilization management and review;
- Quality metrics; and
- Other quality improvement measures.

Health care organizations may argue that many of these processes currently exist in their facilities. The urgency of the Tenet CIA is that these functions must demonstrate their effectiveness and performance — not just their existence.

Compliance officers, quality managers, and risk managers would be well served by a study of this landmark CIA.

**Quality as a Component of Compliance**

When we consider hospital management of regulatory compliance, quality of care, and other risks, it is easy to perceive that most of these large, multi-layered organizations tend to put various types of risk into “silos” or compartments. Hospitals are by nature diverse and highly structured operating environments. They include financial, operations, support, and clinical services. The professionals associated with these various disciplines tend to structure tasks along the lines of their expertise. A strong physician element tends to add a further layer of structure over all things that may be deemed clinical.

The challenge personified by the Tenet CIA is to coordinate and integrate regulatory compliance and quality of care. If spread among other health care organizations, such an effort has the potential to revolutionize how we
Combining Disciplines: Making the Connection

look at compliance, quality, and risk and their impact on a health care organization.

The means to mandate quality performance in health care already exists. Medicare conditions of participation (CoPs) have been found to extend beyond payment requirements to include quality concerns. A fraudulent representation or failed promise to comply with CoPs could make subsequent claims false.

CoP requirements include patient rights (64 FR 36069); quality assessment and performance improvement (68 FR 3435); authentication of verbal orders (42 CFR 482.24(c)(1)), and other pertinent issues. Additional regulatory enforcement authority is found in 18 U.S.C. §1035, False Statements Concerning Health Care. And of course, new P4P programs are expected to carry larger and larger payment incentives and penalties for hospital and physician tracking and failure to track key indicators of quality.

Health care employers also are prohibited from taking action against quality of care whistleblowers. The Patient Safety and Quality Improvement Act of 2005 (42 U.S.C. 299c-21) states in pertinent part:

A provider may not take adverse employment action...against an individual...[b]ased on good faith reported information...[t]o the provider...[o]r to a Patient Safety Organization....

Experience has proven over time that when government enforcement agencies identify a measurable unmet public need, such as quality improvement in health care, and develop over time the means to address the need, enforcement actions predictably follow.

The inescapable conclusion is that compliance has moved from the arena of reimbursement regulation to a new venue that encompasses regulation, quality, and risk as critical components of a combined process.

**STUDYING THE ROOT OF THE PROBLEM**

Separated by organizational silos, many quality managers, compliance officers, and risk managers may not realize they are tackling similar root problems. Similar compliance, risk, and quality concerns can be commonly identified through compliance audits, root cause analysis, or malpractice claims studies.

Several areas of exposure are, not surprisingly, common to each discipline. These include:

- Inadequate medical record documentation;
- Poorly executed patient informed consent;
- Inadequate patient education;
- Poor physician-patient communications;
- Lack of medical necessity for performed medical services; and
- Improper performance of medical services.

In 2006, medical liability insurer American Healthcare Providers Insurance Services (AHPIS, Philadelphia, Penn.) commissioned a study of medical malpractice claims data collected by the Physician Insurer's Association of America (PIAA).

PIAA is an association of 57 malpractice insurers across the United States that collectively provide insurance to 60 percent of U.S. physicians. PIAA has compiled and studied claims data submitted annually by insurers since the mid-1980s.

One goal of the study was to determine whether common risk exposures face medical liability, compliance, and quality disciplines. Study findings were analyzed by senior staff, including a board-certified corporate compliance officer and licensed health care risk manager with hospital, long-term care, and medical practice operations experience, underwriters, and claims managers. The fully developed study data was refined into specialty-specific presentations accredited with the American College of Continuing Medical Education (ACCME) for use as a risk-reduction tool for AHPIS-insured physicians.

The PIAA study examined the following data:

- Leading allegations listed in medical malpractice claims;
Combining Disciplines: Making the Connection

- Frequency (number of claims filed) and severity (indemnity cost);
- Average indemnity payments made for each type of allegation;
- Severity of claims filed in 2005 compared to the average of previous years; and
- Patient conditions and specific procedures or medical events identified in claims.

Some of the data collected over the 10-year period from 1985 to 2005, for all medical specialties, indicate the following:

- Failures to monitor or supervise medical cases resulted in 16,430 cases with a total indemnity payout value of $1.2 billion.
- Medication errors resulted in 9,326 cases with a total indemnity payout value of $369 million.
- Procedures performed when not indicated or necessary resulted in 6,702 cases with a total indemnity payout value of $382 million.
- Failure to communicate or instruct patients resulted in 4,771 cases with a total indemnity payout value of $118 million.7

A study of claims by associated medical or legal issues revealed the following:

- Problems with medical records accounted for 5,051 claims with a total indemnity payout value of $603 million.
- Premature discharge accounted for 2,625 claims with a total indemnity payout value of $242 million.
- Lack of adequate facilities or equipment accounted for 1,985 claims with a total indemnity payout value of $217 million.
- Improper conduct by physicians accounted for 1,943 claims with a total indemnity payout value of $70 million.
- Unnecessary treatment accounted for 1,693 claims with a total indemnity payout value of $118 million.
- Breach of confidentiality accounted for 918 claims with a total indemnity payout value of $8 million.
- Failure to conform with regulations or statutes accounted for 902 claims with a total indemnity payout value of $68 million.
- Pharmacy error accounted for 355 claims with a total indemnity payout value of $18 million.

Managed care referral problems accounted for 276 claims with a total indemnity payout value of $15 million.8

The phrase “total indemnity payout value” refers only to the amounts paid to claimants by jury award or settlement. This does not include any associated costs, such as legal defense or lost time.

Studies conducted internally by AHPI indicate that 112 physician man-hours are needed to participate in defense against one case. This does not include lost productive time associated with rescheduling cases or patient appointments previously scheduled during that 112-hour period.

Those familiar with medical malpractice defense note that notice of depositions or court dates usually are not received with great advance warning. Usually, it is necessary for affected physicians to cancel and reschedule appointments and procedures at the last minute, resulting in greater associated costs for both the medical practice and any affected hospitals. The associated productivity and quality impact of lawsuit defense is significant.

Most risk management issues are directly related to regulatory compliance and quality of care concerns. The issues revealed by many compliance audits are surprisingly similar to those found by quality audits and malpractice risk studies.

THE HAMMER

More than a decade ago, health care organizations slowly began to realize that they must have a corporate compliance program, management of the program by a compliance officer, and essential elements of compliance as outlined in various program guidance documents issued by the OIG. Many compliance officers will remember that a significant educational effort was required to buy in to these efforts at the administrative, board, and physician level.

The importance of instituting compliance programs became clearer when the federal FCA was implicated in noncompliance. As compliance officers know, penalties that can be imposed under the FCA are serious.
Most savvy organizations moved more nimbly to institute compliance programs under the threat imposed by the compliance “hammer” of the FCA. The effect on health care billing and reimbursement systems has been revolutionary, but even with the impact of corporate compliance programs, the OIG still can claim fiscal year 2006 savings or recoveries of $38.2 billion, including $35.8 billion in implemented actions, $789.4 million in audit receivables, and $1.6 billion in investigative receivables.9

Clearly, regulatory compliance investigation exposure is a major source of medical-legal and financial risk for health care organizations. Administration knows that the exposures involved in an implication of the FCA must be carefully avoided, and as with any business, resources are dedicated to addressing these high-severity risk issues.

Many organizations over time have dedicated resource dollars and manpower to initiatives designed solely to serve quality initiatives, but these programs frequently have been geared toward events such as accreditation surveys or addressing immediate problems. Some academic centers and large organizations demonstrate they understand the connection between quality and value by dedicating significant resources to quality. For the most part, however, quality has been commonly relegated to medical staff and nursing quality assurance or quality improvement activities, with too few resources allocated to these efforts.

Under the Tenet CIA, administration should be on notice that quality is a primary and major concern, equal to, and soon to be considered part of, the regulatory compliance program that has in the past protected against allegations of billing and reimbursement fraud and abuse.

An analysis of the medical liability climate clearly illustrates that case frequency (number of cases) and severity (cost of cases) is increasing. Even with a “soft” medical malpractice insurance climate, the average indemnity payment for each type of case allegation has increased in virtually every medical specialty.

For the first time, quality improvement and management is under the same economic “hammer” that regulatory compliance initiatives have been since the passage of the Health Insurance Portability and Accountability Act (HIPAA) in 1996. Another economic hammer that must be recognized is the costs of medical malpractice insurance, representation, and defense.

**The New Direction**

Compliance is now moving in a new, fundamental, and powerful direction. We can reasonably expect that the OIG perceives an opportunity to improve quality of care by implicating the FCA in situations in which quality does not meet standards (such as are outlined or implicated in documents like the Medicare CoPs or accepted as the prevailing standard of care by usage in the community). Using the FCA as an enforcement tool, the OIG is now requiring one large health care organization to demonstrate quality monitoring and improvement.

Many experts believe we soon will see similar elements in corporate integrity agreements for all affected organizations. The extent of OIG expectations will not be limited to those organizations with a CIA, but rather eventually will extend to all health care organizations. Even today, forward-thinking compliance officers see the tacit connection between compliance and quality enforcement.

Compliance and quality management also must include and address medical liability risk and risk management. In an increasingly litigious environment, imagine the potential malpractice exposures faced by a health care provider or organization identified as being under a quality of care compliance audit or prosecution. An even more chilling scenario would involve specific types of medical treatments named in quality investigations. There is significant potential for individual and class action suits, and it is unlikely the well-informed national plaintiff’s bar will fail to see this connection.
The cost of malpractice insurance is growing daily, as is the cost of average indemnity payments for settled or paid claims. This cost directly affects the bottom line of all health care providers and creates additional problems for health care organizations, including availability of physicians, ability to provide services, and physicians and hospitals being simultaneously named in suits.

**The New Conventional Wisdom: Combine Compliance, Quality, and Risk Management**

Compliance professionals must realize that a serious movement has occurred in the industry. We are moving away from the “old” compliance paradigm of managing billing, documentation, and reimbursement systems. The “new” reality is that health care providers are suspected of not only incorrectly billing, but also providing quality of care that is below acceptable standards. Compliance as a profession must move toward enforcing quality delivery of medical services that also are correctly accounted for, documented, and billed.

Compliance officers typically are highly accountable individuals. This reflects the training and the standards of the profession. The new compliance and quality paradigm will demand that they become accountable for a new arena previously reserved for clinical peer review, quality assurance, or quality improvement programs. Inserting the compliance program in these areas will require reeducation for management, nursing, and physicians. It also will require compliance-type accountability systems.

Auditing and monitoring systems in traditional hospital quality assurance, quality improvement, and peer review have been subject to limited funding and staffing. As they directly affect clinical practice, they have been managed by clinicians or clinical committees that have relatively limited enforcement capability.

The self-policing abilities of peer review and medical staff are frequently affected by political and relationship considerations. The result of these functional impediments is that quality programs are usually less effective than quality managers would prefer. In short, quality initiatives in many health care organizations do not have the “teeth” that a robust compliance process enjoys through application of the FCA and other federal and state laws and regulations.

Many believe the fundamental difference between a traditional hospital quality program and a compliance-based quality program is that compliance-driven quality programs have a better chance of positively influencing behavioral change in the organization, from the top down. Over time, the OIG, CMS, and DOJ will continue to pursue and implement their interest in monitoring, measuring, and enforcing quality. This likely will take the form of additional quality-related corporate integrity agreements and compliance investigations that consider quality of care as a component of false claims.

To date, the OIG and DOJ, along with state Departments of Health, have conducted quality-focused reviews of industry segments such as long-term care, home health, and hospice. Clearly, the Tenet CIA puts compliance officers on notice that hospitals and medical practices will be the next focus of such reviews. Under the Deficit Omnibus Reconciliation Act of 2005 (DRA), states are expected to implement their own False Claims Acts and may enjoy the opportunity to retain part of the funds collected by state FCA investigators.

**Ahead of the Curve?**

Are compliance officers who seek to implement quality and compliance processes too far ahead of the “curve” to win support and acceptance from administration and their clinical colleagues? In this case, it is better to be ahead of the curve than behind it. The Tenet CIA serves as a reminder that the OIG, CMS, and DOJ are increasingly quality-focused organizations.

The quality actions of the OIG in the new Tenet CIA represent a regulatory agency
Combining Disciplines: Making the Connection

approach to quality of care in a major U.S. hospital system. This quality focus has been seen during investigations in some health care industry segments but not to such a large degree in hospitals and medical practices. Many experts are convinced that a combined quality and compliance focus will be seen in the regulatory and investigative future at both the state and federal level.

For hospitals and medical practices, the new Tenet CIA represents a great learning opportunity. A review of the CIA and the related appendices reveals a number of lessons. Hospitals and physicians should be alerted to the implications of a quality agenda in corporate integrity agreements. This agenda not only will affect the CIA organization but has the potential to impact the health care industry as a whole across all segments of care.

Given this information, compliance officers now have a perfect opportunity to consider the OIG, DOJ, and CMS’ future quality and compliance actions. They must act decisively to prepare compliance programs to review quality as well as billing, documentation, and reimbursement.

Compliance officers who choose to wait with regard to implementing quality of care standards have another consideration. The DRA calls for states to develop their own False Claims Acts and allows states to retain a portion of recoveries from investigations. This is a powerful incentive for state health departments and attorneys general to move forward with their own quality and compliance investigations.

When convincing administration to properly fund quality, risk, and compliance, we would do well to paraphrase Philip Crosby, one of the early leaders in American quality thinking:

Quality is Free. Every dollar we don’t spend doing something over or correcting something done wrong is a dollar that goes straight to the bottom line.

Endnotes:
Teleradiology: Compliance Concerns and Solutions, Part III

Many of the Challenges in Teleradiology Can Be Addressed Through a Series of Practical Strategies

Fay Rozovsky / Susan T. Goodwin

This article is part three of a three-part series on teleradiology and provides information on medical liability and jurisdictional issues, clinical communications, documentation practices, billing and coding, and quality assurance processes and accountabilities in teleradiology.

MEDICAL LIABILITY AND JURISDICTIONAL ISSUES IN TELERADIOLOGY

If a misadventure occurs that involves a misdiagnosis or missed diagnosis on the part of a teleradiologist, the patient is apt to file a claim against the hospital, the ambulatory care center, or the local radiology group. The reason is simple: the patient looked to the institution or radiology group for care. The teleradiologist may be named a third-party defendant.

While the teleradiology vendor may agree to be contractually obliged to participate in professional liability claims stemming from its provision of interpretive services, there are some challenges to this approach. How will one serve notice of a claim on a teleradiology group based in India or Australia? Does the vendor have a local agent for service of process? Even if the vendor admits to its responsibility for the misadventure, how can it be compelled to satisfy a judgment?

What if the vendor's local professional liability insurance coverage does not include errors and omissions emanating from teleradiology services? What if the teleradiology group has shared limits among several radiologists and the group has exhausted the limits of the policy?
Strategies
There are some practical strategies to address these issues. One is to avoid use of teleradiology vendors who are not subject to the jurisdiction of American courts. Another strategy is to require by contract designation and maintenance of a U.S.-based agent for service of process. The contract also can serve as the vehicle for another strategy, namely to require the teleradiology vendor to carry professional liability insurance with appropriate limits for each radiologist offering services to patients in the United States.

The contract can be very specific, describing the type of carrier (well rated), providing a verified original declaration page from the insurance policy, and insisting that the teleradiology group's insurer pay all costs associated with defense of the claim. A consent to settle provision also may be a prudent strategy in crafting the contract with the teleradiology group.

Another point merits consideration. Since litigation may go beyond traditional professional liability, thought should be given to other types of claims that may arise from teleradiology. Breach of contract, deceptive trade practices, breach of confidentiality, and breach of privacy should be considered when drafting the contract and the specifications for insurable items for which the teleradiology vendor should be required to obtain adequate levels of coverage.

Clinical Communications in Teleradiology
As with other areas of health care delivery, teleradiology is at risk for a breakdown in communication. Teleradiologists trained abroad and unfamiliar with American idioms or phraseology may use terms that do not convey the urgency of a situation or the importance of an area detected on a diagnostic image. For their part, American care providers who initiate the request for “after hours” teleradiology services may not appreciate the communication divide. They may draw the wrong inference after reading a radiologist’s report from abroad. That a diagnostic image is degraded during transmission can contribute to the problem with a less-than-refined view leading to an ambiguous report.

A key area in clinical communications is timing. A “critical” diagnostic image must be read within a defined timeframe in order for the radiologist to provide important information to the attending care provider. The failure to communicate the urgency of the situation can lead to a delay in care and patient injury.

Sometimes a delay in care is occasioned by equipment failures or transmission line problems. Trying to work on this problem can delay communication of critical results, again leading to patient injury. This is the type of problem that can happen with any type of telemedicine — not just teleradiology, whether domestic or international.

Health care risk managers and patient safety experts realize that communication breakdowns account for many patient injuries and also are a major cause of litigation. Lack of time sensitivity with respect to diagnostic test results also is important for purposes of compliance with the conditions of participation for hospitals under Medicare and Medicaid.

Strategies
There are a number of practical strategies to consider to address clinical communication concerns in all domestic and international models of teleradiology. One strategy is to develop a consistent taxonomy of terms or “universal” language to be used by teleradiologist and originating sites in communicating diagnostic imaging information and results. The framework for these terms may be set by radiologists, and the implementation of the framework may be via contract.

A second strategy is to develop a standardized method for reporting results. Taking this step can obviate ambiguous or unclear language in teleradiology reports that offer little assistance to care providers at the originating site. Once again, the con-
tract can be a tool for enforcing this standardized approach to reporting.

A third strategy is to set a norm for timeliness of communication. Reporting of critical diagnostic imaging results should have a clear timeframe that is incorporated into the contract and monitored for compliance via quality review. Originating site leaders should make it very clear that there is “zero tolerance” for untimely reporting of diagnostic imaging reports by teleradiology contractors. For non-critical diagnostic imaging reports, specific time thresholds should be established and enforced.

Finally, redundancy should be built into the system for those occasions in which there is a failure of the primary method of communicating diagnostic imaging results. Thus, if the primary mechanism is email, the back-up strategies may be fax transmission or telephonic reporting that is then augmented by transmission of hard-copy or e-copy data when the primary system is back up and running. From a risk management and quality perspective, the back-up systems should be tested from time to time to make certain that these “safety net” approaches will be effective.

**Documentation Practices and Teleradiology**

There are some very practical concerns that involve documentation generated in the course of teleradiology. These concerns are equally important for domestic and international models of teleradiology.

With many if not most overnight teleradiology programs, the initial diagnostic imaging report is considered a “preliminary reading” until there is an over read by a radiologist at the originating site. In the overnight hours, other care providers rely upon the preliminary report to develop a care plan and order additional tests and medications. The preliminary report also may suggest — as in the case of Ms. Wherton at the beginning of this article series — that a suspected health concern should be ruled out. The result may be to follow a more conservative approach in treatment.

Local care providers may not know until the over read is completed that there was a misdiagnosis or missed diagnosis based on the preliminary reading. By that stage in the patient’s treatment, irreparable harm may have occurred, setting the stage for potential litigation if not regulatory review.

When there is a difference of opinion, which reading constitutes “the” report? Is it the preliminary diagnostic interpretation performed by the teleradiologist? Or, will it be the over read report? Will the local radiologist sign the preliminary diagnostic imaging report even though he or she disputes the finding? Will the local radiologist add comments to the preliminary report to explain the disputed finding? Or, will the local radiologist sign just the over read and use that report as the basis for coding and billing?

For health lawyers and compliance officers, disputed preliminary findings can create serious concerns. The preliminary report may be evidence of substandard care, forming the basis for malpractice litigation. If it is part of a continuing trend in which there are major quality and accuracy variances between preliminary reports and over reads, and nothing is done to address these concerns, will it be evidence that can be used for regulatory enforcement purposes under the conditions of participation against the hospital?

There are many thorny issues associated with use of preliminary reports. If a preliminary report is overridden based on an interpretation by a local radiologist, what should become of the preliminary report? Will some think it prudent to destroy that report, fearing that it serves as evidence of a breach of a standard of care?

If such thinking prevails, could it not set the stage for a claim of spoliation of evidence in subsequent litigation when the plaintiff seeks through discovery to obtain a copy of the preliminary report? Moreover, would destruction of the preliminary report hamper efforts to bill correctly for the diagnostic imaging service?

Another concern is retention of diagnostic imaging information and results. The
length of time for retaining documentation will be influenced by many considerations, not just the potential for litigation. Hence, if a longitudinal study is being conducted using teleradiology results, the retention time may be far longer than that established for medical malpractice exposure.

Concerns about tax liability also may trigger longer retention periods than that which applies to medical malpractice. Thus, it is important to think about the various uses of teleradiology images, storage, access, and retention periods.

**Strategies**

There are a number of practical strategies to consider when addressing documentation practices in teleradiology. One is to assemble a team of key stakeholders to obtain valuable input on processes that can serve as the basis for a cogent policy and procedure. Radiologists, corporate compliance, risk management, quality professionals, and legal counsel can help in this regard. Health information management professionals can offer practice guidance on protocols for diagnostic imaging storage, retention, and retrieval.

A second strategy is to establish a process for working with preliminary diagnostic imaging reports. Should an over read reveal differences in interpretation, the process should address this issue. One way to manage the issue is to have the first reading clearly labeled “Preliminary Interpretation” and provide an explanation regarding the scope of the reading.

A second part to the same document or report may be labeled “Final Interpretation.” Without appearing judgmental or argumentative, the final interpretation can provide a factual explanation regarding the difference in opinion. Taking this approach obviates the risk of record spoliation that emanates from destruction of the original report.

A third strategy is to curtail the timeframe between a preliminary diagnostic imaging report prepared via teleradiology and the over read or final interpretation.

Because subtle aspects of the diagnostic image may experience degradation in transmission, the sooner the over read the better in making certain that accurate information is provided to the attending physician.

Careful thought must be given to managing the uses and retention of the preliminary teleradiology report and the over read or final interpretation. A concerted effort is in order to make certain that the process used to support patient care also reinforces corporate compliance, quality improvement, and risk reduction activities.

**BILLING AND CODING**

One area ripe for corporate compliance intervention is establishing a framework for billing and coding for teleradiology services. Lacking the requisite knowledge on the subject can expose a health care entity to needless regulatory difficulties.

CMS is quite explicit on the subject. Other than a few narrowly defined exceptions, Medicare will not pay for services performed outside the United States. This includes radiological interpretations performed by radiologists who hold licensure in an American state.

The payment prohibition has been reiterated in the Medicare Benefits Policy Manual, and it is significant. To bill for a service that is prohibited by Medicare can set the stage for a false claim and possibly fraud and abuse. A recent publication from CMS clarifies the applicability of the payment prohibition:

Payment may not be made for a medical service (or a portion of it) that was subcontracted to another provider or supplier located outside the United States. For example, if a radiologist who practices in India analyzes imaging tests that were performed on a beneficiary in the United States, Medicare would not pay the radiologist or the U.S. facility that performed the imaging test for any of the services that were performed by the radiologist in India.
This change has raised concern among compliance professionals and health care attorneys as they differ about the application of the recent transmittal language. Some fear that it casts a shadow on billing Medicare for teleradiology services that involve even a portion of a service completed by a radiologist overseas. Others do not share this concern. That there is such a difference of opinion in the meaning of the transmittal suggests that CMS may have to issue further explanatory language. One item is clear, however: serious risk exposure exists for those hospitals that do not comply with acceptable procedures when billing and coding for off-shore teleradiology services.

What is not addressed, however, is a very practical concern. If there is a six to 10-hour delay between the initial reading and the over read, should a payer be billed for this “service” if it involves a delay in care and a resulting adverse outcome? In other words, would this constitute substandard care for which it is inappropriate to bill to the payer?

Aside from concerns about the possibility of a delay in appropriate care, the American College of Radiology (ACR) has raised an interesting ethical issue regarding a physician “signing off” on and billing for an interpretation made by another physician. In a May 2006 pronouncement, ACR said:

It is unethical and likely fraudulent for a physician who has not personally interpreted images obtained in a radiologic examination to sign a report to take attribution of an interpretation of that examination rendered by another physician in a manner that causes the reader of a report to believe that the signing radiologist was the interpreter.6

Thus far, major payers have not indicated whether there is agreement with ACR’s statement. Certainly, if payers did agree, it would have a chilling effect on the practice of American radiologists conducting over reads of international teleradiology reports, particularly when the incentive is the ability to bill for the service.

**Strategies**

Billing and coding for teleradiology over reads merits careful review. A key strategy is to enlist the help of the corporate compliance officer and those responsible for billing and coding. For larger radiology groups that rely upon a third party to manage billing services, a related strategy is to work with them and legal counsel to develop an acceptable billing practice.

Another strategy is to determine what should be done in those instances in which a delay or poor interpretation does not rise to the level of quality care sufficient to bill the payer. A thoughtful discussion is in order regarding the propriety of recording the patient care encounter but not billing for it based on quality considerations. Once again, a good approach is to discuss this issue with the compliance officer and legal counsel.

Finally, hospitals, ambulatory care centers, and radiology groups should ask the compliance officer and legal counsel to keep them up to date on billing and coding developments in this area. The recent Medicare policy changes, future CMS interpretations, and legal rulings should be considered in maintaining acceptable billing practices for international teleradiology services. Such an approach also applies to billing private payers.

**Teleradiology Quality Assurance Processes and Accountabilities**

Teleradiology services require alignment with federal rules that address quality assurance and performance improvement. That the last patients’ rights standard promulgated by CMS involves quality assurance and performance improvement is significant. At the core of the requirement is accountability placed squarely on the shoulders of those in governance. Beyond government rules, accreditation standards also set a framework for accountability, particularly with respect to contracted services.
Governance Responsibilities
The hospital Conditions of Participation (CoPs) state that radiological services may be provided by a hospital directly or through a contractual arrangement. The expectation is that the same standards apply regardless of direct provision or contracted radiological services. Additionally, the standards require a hospital's governing body to be responsible for services provided under a contract.7

The interpretive guidelines specify that the governing body has the responsibility for assuring that hospital services are provided in compliance with the Medicare conditions of participation and in accordance with acceptable standards of practice, whether the services are provided directly by hospital employees or indirectly by contract. CMS requires that a hospital's governing body must take actions through the hospital's quality assessment and performance improvement (QAPI) program to “assess...services provided under contract, identify quality and performance problems, implement appropriate corrective or improvement activities, and to ensure the monitoring and sustainability of those corrective or improvement activities.”8 The interpretive guidelines for radiology services also specify that the hospital’s radiological services, including any contracted services, must be integrated into its hospital-wide QAPI program.9

Quality Assurance and Performance Improvement
The CMS condition of participation for quality assessment and performance improvement specifies that the hospital must develop, implement, and maintain an effective, ongoing, hospital-wide, data-driven quality assessment and performance improvement program. The hospital’s governing body is required to ensure that the QAPI program reflects the complexity of the hospital’s organization and services, involves all departments and services (including those services furnished under contract or arrangement), and focuses on indicators related to improved health outcomes and the prevention and reduction of medical errors.10

Joint Commission Requirement for Oversight of Contract Services
In the Joint Commission standards for hospitals, various Leadership Standards and Elements of Performance, when viewed together, establish concepts that relate to requirements for the hospital to perform oversight of contract services. Standard LD.3.30 requires that “a hospital demonstrate a commitment to its community by providing essential services in a timely manner.”

The Elements of Performance include diagnostic radiology as an essential service. The rationale for this standard requires that leaders conduct planning (1) to determine which services are essential and whether the hospital will provide such services directly or through referral, consultation, contractual arrangement, or other agreements; and (2) to establish timeframes within which these patient care services will be provided.

Standard LD.3.20 requires that “patients with comparable needs receive the same standard of care, treatment, and services throughout the hospital.” The rationale statement for this standard explains that “leaders must make sure that factors such as different individuals providing care, treatment, and services, different payment sources, or different settings of care do not intentionally negatively influence the outcome” of care (emphasis added). Based on this standard, it could be expected that a hospital shall ensure that the level of care and services provided by an after-hours teleradiology provider will be comparable in timeliness and quality to that of the radiologists providing services at other times of the day.

Standard LD.3.50 requires that “services provided by consultation, contractual arrangement, or other agreements are provided safely and effectively. The Elements of Performance for this standard require that (1) sources of contract services be approved
by hospital leaders, (2) the medical staff advise the hospital's leaders on sources of clinical services to be provided by contract, (3) the nature and scope of services provided by contract be defined in writing, (4) contract services meet applicable Joint Commission standards, (5) the hospital evaluate the contracted services to determine whether they are being provided according to the contract and at the level of safety and quality the hospital expects, and (6) the hospital retain overall responsibility and authority for services furnished under a contract.

Specific standards also require individual teleradiologist performance to be measured and compared. With the publication of new medical staff standards for 2007, the Joint Commission introduced requirements for conducting ongoing evaluation that is used for ongoing privileging decisions [MS.4.15, MS.4.30, MS.4.40].

Based on both CMS and Joint Commission requirements, QAPI activities must include teleradiology services used by the hospital. When services are provided after hours by a teleradiology group, comparative data should be used to evaluate the performance of the teleradiologists as compared to the radiologists providing services during the day to ensure the same level of quality. Additionally, the performance of individual teleradiologists should be measured for ongoing evaluation as required by the Joint Commission.

**Strategies**

One of the traditional approaches to a review performance for radiology services has been to measure and evaluate the rates of disagreement in imaging interpretations. The results should be stratified by type of study; for example, plain radiography, fluoroscopy, angiography, ultrasound, computed tomography, mammography, nuclear medicine, and magnetic resonance imaging. To the extent that teleradiologists provide interpretation for the different types of studies, the data should be further stratified and evaluated to compare the performance of teleradiologists with that of resident radiologists.

Disagreement rates should be within acceptable limits, and the rates of disagreement for interpretations by teleradiologists should not be significantly statistically higher without triggering further investigation to identify causes and to take steps to improve performance. In a study published in 1998,12 a review of over 11,000 images read by 35 radiologists in six radiology groups found a mean rate of interpretation disagreement of 4.4 percent; only one radiologist had a mean rate above 8 percent. Qualitative analysis of the interpretation errors revealed a mean rate of 3.0 percent of errors that were considered to be below an acceptable standard of care.

It might be expected that these rates would be lower with the use of digital imaging technology (PACS) if transmission capabilities and equipment used to view the images are at appropriate standards. In one study of interpretations of computed tomography (CT) studies, a comparison was done between the official in-house diagnostic report and the preliminary readings transmitted from the in-hospital PACS system to a radiologist in Bangalore, India. Out of 106 cases, there was discordance between the official in-house diagnostic report and the preliminary readings in 20 (19 percent) of the cases; however, on subsequent review the teleradiology report was found to be correct in 13 of these, so the final rate of disagreement was 6.6 percent.13

Because teleradiology services are used in many hospitals to improve timeliness of interpretations, hospitals should include in their evaluations some measurement of interpretation timeliness, such as report “turn around times” (TATs). Actual performance should be compared to performance expectations. The hospital should expect that teleradiology TATs will be within expected range.

Joint Commission Standard LD.3.15 requires planning and assessment by hospital leaders with regard to patient flow, including a requirement to measure support
service processes that impact patient flow.\textsuperscript{14} Of specific interest to the hospital should be how well use of teleradiology services enhances timeliness of services and facilitates patient flow.

The Joint Commission also has established a national patient safety goal (NPSG) that requires hospitals to measure, assess and, if appropriate, take action to improve the timeliness of reporting and the timeliness of receipt by the responsible licensed caregiver of critical test results and values.\textsuperscript{15} Radiology reporting must be included when defining critical test results and the acceptable length of time between availability of a critical result and receipt by the responsible licensed caregiver.

The NPSG also requires that a hospital collect data regarding timeliness of reporting, assess the data, and take action to improve. If the hospital uses teleradiology services after hours, data about timeliness of reporting of critical test results by the teleradiology service should be measured and compared with hospital expectations and with timeliness of reporting by radiologists during other times of the day.

Other QAPI activities or strategies to consider are unique to teleradiology. The Royal College of Radiologists in the United Kingdom has considered concerns about linguistic differences when using teleradiologists.\textsuperscript{16} The Royal College recommended that language proficiency necessary for performing professional activities should be required for licensure to practice.

The College also recommended careful audits of foreign-language radiologists to ensure accuracy of conveyed messages. In a recent article in the \textit{New England Journal of Medicine}, author John F. Bruzzi described his experiences as an Irishman pursuing a radiology fellowship in France. He described how language is the "lifeblood" of radiologists and how language barriers resulting from his limited proficiency in French reduced his ability to convey his interpretations using words for balance, weighing diagnostic probabilities, and instead forced interpretations that gave the impression of diagnostic certainty.\textsuperscript{17} QAPI data regarding the rates of disagreement in imaging interpretations should be evaluated to determine if the variable causing any unacceptable rate might be due to language differences.

Another strategy is to inquire whether the teleradiologist is familiar with the patient population and health status and conditions. The example used by British authors is consideration of whether a southern European radiologist reporting a preoperative chest radiograph obtained in Portsmouth, United Kingdom, was aware of the higher-than-average risk of asbestos exposure.\textsuperscript{18} QAPI data regarding the rates of disagreement in imaging interpretations should be evaluated to determine if the variable causing any unacceptable rate might be due to limited knowledge of the patient population and their environment.

Finally, a comprehensive QAPI strategy includes use of relevant quality control data and is required by the Joint Commission. [PI.1.10]\textsuperscript{19} Quality control activities should include monitoring the performance of teleradiology equipment and data transmission quality. QAPI data regarding the rates of disagreement in imaging interpretations should be evaluated to determine if the variable causing any unacceptable rate might be due to teleradiology equipment or transmission capabilities.

**Conclusion**

Teleradiology offers a promise of prompt, cost-effective, efficient, accurate, and useful diagnostic imaging information to assure quality, safe patient care. To realize this promise, however, many challenges must be addressed. Key hurdles include contracting, consent, confidentiality, licensure and credentialing, insurance coverages, regulatory compliance, billing, coding, and accreditation issues.

Through a series of practical strategies, many of these challenges can be addressed. A team effort will be useful, enabling key stakeholders to share their insights in designing a sufficient program for teleradiology services.
A checklist provided in Appendix A that offers useful considerations when designing a compliance-based approach to teleradiology services.

**Endnotes:**

2. CMS, *Survey Protocol, Regulations, and Interpretive Guidelines for Hospitals, in State Operations Manual,* App. A, §482.24(c) (Rev. 1, May 21, 2004), available at http://www.cms.hhs.gov/manuals/downloads/som/07ap_a_hospitals.pdf (“Patient medical record information, such as, laboratory reports, test results, consults, assessments, radiology reports, dictated notes, et cetera must be promptly filed in the patient’s medical record in order to be available to the physician and other care providers to use in making assessments of the patient’s condition, to justify continued hospitalization, to support the diagnosis, to describe the patient’s progress, and to describe the patient’s response to medications, interventions, and services, in planning the patient’s care, and in making decisions on the provision of care to the patient.”) (emphasis added)
7. 42 C.F.R. §§482.12, 482.26; see also CMS, supra note 2 at App. A.
8. See CMS, supra note 2 at §482.12(e).
9. See id. at §482.26.
10. See id. at §482.21.
15. Id. at Chapter on National Patient Safety Goals, Requirement 2C.

---

**Appendix A**

**Checklist for a Compliance-Based Approach to Teleradiology Services**

- Determine which teleradiology model is consistent with applicable state law.
- Conduct a prospective failure mode and effect analysis to determine potential clinical, quality, patient safety, and regulatory challenges to use of possible teleradiology models. Decide which model will be the most cost effective.
- Develop a comprehensive teleradiology contract that addresses the following:
  - Scope of services
  - Service providers
  - Equipment standards
  - Transmission standards
  - Communication standards
  - Timeliness of reports and “critical diagnostic imaging results”
  - Standards for interpretive reports
  - HIPAA privacy and security compliance
  - Quality review
  - Record access
  - Record retention
  - Right to refuse a successor vendor when the contractor sells, assigns, or participates in a merger with another teleradiology company
  - Notification provisions

---
Develop a credentialing process that complies with applicable state and federal laws, accreditation standards, and ACR guidance on teleradiology credentialing, including:

- Verification of identity
- Primary source verification of critical biographical, licensure, and professional qualifications for teleradiology
- Verification of specialty board certification by the American Board of Radiology
- Requirements for disclosure of any challenges to licensure, adverse actions involving licensure in any jurisdiction, any adverse actions regarding medical staff membership or clinical privileges in any location
- Verification of adequate malpractice insurance coverage
- Verification of clinical competence as a teleradiologist
- National Practitioner Data Bank query
- Federation of State Medical Board query
- Review of the OIG and General Services Administration exclusion lists if the services are to be billed to a federal program and a check of the state exclusion list if services will be billed to Medicaid and if the state maintains an exclusion list
- A signed acknowledgement from the teleradiologist that he or she agrees to abide by the medical staff bylaws, rules, regulations, and hospital policies, including any privacy policies and agreement to release the hospital and all individuals involved in credentialing from civil liability
- Review and a recommendation from the department chairman responsible for radiology services, if the medical staff is departmentalized
- Review and a recommendation from the hospital’s medical executive committee
- Review and approval by the hospital’s governing body

Establish a process for granting privileges to teleradiologists and mid-level practitioners

- Develop a process to achieve compliance with accreditation standards
- Develop a process to achieve compliance with the CoPs
- Include a requirement for patient consent to participate in teleradiology and follow legislative requirements where provisions are established in the law for consent to such services
- Develop a process for compliance with HIPAA privacy
- Develop a process for compliance with HIPAA security

Develop a process for compliance with ACR technical standards for teleradiology, including equipment specifications for teleradiology

Delineate required insurance coverages and both individual and aggregate limits for all types of potential litigation associated with the delivery of teleradiology services

- Require original declaration page from the insurance policy
- Require the contracted teleradiology group to pay costs associated with defending a claim
- Require a consent to settle
- Develop a universal language to be used by teleradiologist and originating sites in communicating diagnostic imaging information and results
- Standardize methods for reporting results
- Establish and maintain through a compliance-based quality review timeframes for critical diagnostic imaging test results
- Establish requirements for diagnostic imaging storage, retention, and retrieval
- Establish a process for working with preliminary diagnostic imaging reports, including retention and reconciling variances with final over read interpretations
- Establish a regulatory compliance process for billing and coding
- Develop a process for complying with QAPI
Allied Health Professionals Should Provide Only Those Services That Are Within Their Scope of Practice

Even Though Compliance Officers May Feel They Have a Handle on This, Errors Still Persist

Georgette Gustin

For most organizations, the volume of patient encounters has increased while reimbursement continues to steadily decline. To remain competitive, as well as increase patients’ access to care and address physician workload, many organizations began utilizing various nonphysician practitioners or allied health professionals, such as nurse practitioners (NPs), physician assistants (PAs), and certified nurse midwives (CNMs), et cetera.

Understanding the types of services that each allied health care professional within your organization can perform is critical for a variety of reasons, including:

- Quality of care;
- Patient safety;
- Medical malpractice;
- Public reputation; and
- Reimbursement.

While most compliance officers may feel they have a good handle on this, there are still far too many errors that are continuing to surface. Practicing outside of one's scope of practice can create a whole host of issues, as well as lead to unknowing submission of false claims.

Often these types of scenarios can go on for months or years with no one even giving it a second thought. Generally it takes a patient or employee complaint, payer billing inquiry, follow-up on a denial in the business office, compliance audit, or risk assessment (whether conducted internally or externally) to identify these situations. Unfortunately, by the time this occurs, upwards of several hundreds or thousands of claims (i.e., dollars) could have been submitted and paid.
Let’s review one of the Office of Inspector General (OIG) work plan focus areas for fiscal year 2007: services and supplies rendered “incident-to” a physician’s service. This particular area has been an initiative directed at physicians and other professionals a total of five times since the OIG first began publishing its work plan in 1997. Obviously, there has been much confusion around the complex Medicare regulations that govern the “incident-to” services.\(^1\)

As a result of the 1997 Balanced Budget Act, most organizations first became familiar with the term “incident-to,” which allowed NPs and PAs to obtain their own unique provider identification number (UPIN) for Medicare billing purposes. This change allowed NPs and PAs to submit claims for services they rendered and receive 85 percent of the Medicare physician fee schedule amount (under specific circumstances), or submit their services “incident-to” the physician’s services and be paid at 100 percent of the fee schedule amount.

Given the financial challenges that most organizations were facing, most opted to continue submitting the non-physician practitioners services under the “incident-to” provisions. Most, however, did not develop any processes to monitor their compliance with these provisions, and business continued as usual.

It was not until Medicare revised the provider-based requirements that organizations once again began to analyze their outpatient settings. As such, many began reviewing the reimbursement associated with a physician clinic versus an outpatient hospital department. This was due to the changes in the provider-based regulations and the implementation of ambulatory payment classifications (APCs) in August 2004. In addition, in its 2004 work plan, the OIG published a new initiative directed toward physicians and other professionals around place of service (POS) errors.\(^2\)

For Medicare purposes, it is extremely important to understand the setting in which a service was rendered. Each setting is distinguished by a POS code that is used on the claim form to communicate in which type of setting the procedure was furnished. (See Figure 1). The POS is a two-digit numeric code that is required on the CMS 1500 claim form.\(^3\) Using the wrong POS code can have a direct impact on how payments are calculated by Medicare.

The Medicare physician fee schedule is based on the resource based relative value system (RBRVS), which includes the malpractice, work, and practice expense relative value units (RVUs).\(^4\) Depending on the type of procedure (i.e., CPT® code) some physician professional services have separate payments when provided in a facility (provider based) versus nonfacility (physician clinic or office) setting. Under the physician fee schedule, Medicare refers to this as the “Site of Service Differential.”\(^5\)

Part of the problem has been caused by a lack of knowledge, processes, or workflow deficiencies around which physician professional services are allowed. In addition, failure to align permitted procedures with the appropriate POS codes, as well as using various types of allied health professionals, has led many organizations into preparing self-disclosures to the OIG. Many of these self-disclosures arose from situations in which the organization was billing for all services “incident-to” physician services in a provider-based clinic or POS 22.

It is important to keep in mind that the “incident-to” provision is not applicable in a provider-based clinic, as in this setting the organization is split billing.
and the physician is only receiving payment for the professional component (PC). Therefore, the payment for the facility or technical component (TC) is reported on the UB92 (or new UB04) claim form.

Conversely, many organizations met the provider-based status but reported the professional physician services on the CMS 1500 claim using the POS 11. While the POS 11 code (physician clinic) permits the use of “incident-to” services, the issue became that the actual services should have been reported using the POS 22 code. Therefore, the claims that had been submitted incorrectly with the POS 11 code on the CMS 1500 claim form were reported and paid on the total or “global” component. The global component is a higher payment within the RBRVS as it contains the malpractice, expense, and work RVUs, whereas the POS 22 code does not include the “practice” expense RVU; hence comes the “site of service differential” discussed earlier.

Figure 2 includes a sample of HCPCS CPT® codes that contain a “global,” “technical” (TC), and “professional” (-26) component derived from the Medicare physician fee schedule database for 2007.

It is important to note that snafus associated with not using the appropriate licensed and credentialed professionals are not limited to NPs, PAs, or CNMs, nor are they limited to the incorrect use of POS codes 11 and 22. Other allied health care professionals are often used in both facility and nonfacility settings. Such professionals include:

- Audiologists;
- Dieticians;
- Licensed practical nurses (LPNs);
- Medical assistants;
- Psychologists;
- Social workers; and
- Technicians (orthopaedic, ophthalmology, et cetera).

Let’s examine a few scenarios that highlight some of the potential errors in more detail.

For compliance purposes, you are conducting a coding and documentation assessment of physician clinic services. The claims have been billed, and you have a copy of the medical record documentation for the date of service under review, a copy of the encounter form, a printout of the CMS 1500 claim form from the billing system, and the explanation of benefits (EOB). Upon analyzing the medical record, you determine that the only documentation present was for an injection that was rendered by the LPN.

You refer to the copy of the encounter and note that the service was billed under the physician name. Therefore, it appears that the service was billed under the “incident-to” provisions, and at this point you believe everything looks good.

To complete your analysis, you review the EOB and identify that the POS code used on the claim was POS code 22 (provider-based facility). You know that “incident-to” services are not permitted in this setting, so you document your observations and move on to the next record in your sample. You go through the same process as described above; however, when you get to the EOB form, you note that the POS code was 11.

<table>
<thead>
<tr>
<th>HCPCS</th>
<th>MOD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>70120</td>
<td>TC</td>
<td>X-ray exam of mastoids</td>
</tr>
<tr>
<td>70120</td>
<td>26</td>
<td>X-ray exam of mastoids</td>
</tr>
<tr>
<td>91010</td>
<td></td>
<td>Esophagus motility study</td>
</tr>
<tr>
<td>91010</td>
<td>TC</td>
<td>Esophagus motility study</td>
</tr>
<tr>
<td>91010</td>
<td>26</td>
<td>Esophagus motility study</td>
</tr>
<tr>
<td>93307</td>
<td></td>
<td>Echo exam of heart</td>
</tr>
<tr>
<td>93307</td>
<td>TC</td>
<td>Echo exam of heart</td>
</tr>
<tr>
<td>93307</td>
<td>26</td>
<td>Echo exam of heart</td>
</tr>
<tr>
<td>94060</td>
<td></td>
<td>Evaluation of wheezing</td>
</tr>
<tr>
<td>94060</td>
<td>TC</td>
<td>Evaluation of wheezing</td>
</tr>
<tr>
<td>94060</td>
<td>26</td>
<td>Evaluation of wheezing</td>
</tr>
<tr>
<td>99211</td>
<td></td>
<td>Office/outpatient visit, est</td>
</tr>
<tr>
<td>99212</td>
<td></td>
<td>Office/outpatient visit, est</td>
</tr>
<tr>
<td>99213</td>
<td></td>
<td>Office/outpatient visit, est</td>
</tr>
<tr>
<td>99214</td>
<td></td>
<td>Office/outpatient visit, est</td>
</tr>
<tr>
<td>99215</td>
<td></td>
<td>Office/outpatient visit, est</td>
</tr>
</tbody>
</table>

Allied Health Professionals Should Provide Services within their Scope
Something does not seem quite right at this point, so you refer to the dates of service on claims, as well as the payers and whether or not each claim had been paid or denied. In reviewing the EOBs in greater detail and through further investigation with the business office personnel, you find that the data entry personnel were changing the POS codes in order to get paid.

The biller had no idea that what he was doing would create a problem; he was simply doing his job, which was to submit the bills and work the denials. In this scenario, had the process for conducting the compliance coding and documentation review not included examining a sample of records that had been previously billed, the EOB would not have been included as a source document in the analysis. Therefore, the error could have gone undetected for quite some time, as the reviewer would have assumed that everything was accurate. It appeared based on the documentation and encounter form that the service had been billed under the “incident-to” provisions in the appropriate setting, which was not the case after all.

Other errors have occurred when services were rendered by allied health professionals in either the POS code 23 (emergency department) or POS code 21 (hospital inpatient) settings and were billed incorrectly under the “incident-to” provisions in the appropriate setting, which was not the case after all.

In many cases, these errors were not identified until the medical record documentation was under review, and the only documentation present for the date of service for which the bill was submitted was for a service rendered by an “orthopaedic technician.” In this situation, the claim had been submitted under the orthopaedic surgeon’s provider identification number (PIN) as an “incident-to” service. Over the years, there have been many situations in which NPs, PAs, or other allied health professionals have rendered services in the emergency department that were billed under a physician’s name — without the physician’s knowledge.

Based on Medicare’s primary care exception rules, residents can see patients and their services can be billed under the teaching physician’s PIN, under specific circumstances and requirements. In one situation, however, residents’ services had been submitted; but the residents were not properly licensed at the time of the claim, nor had they been appropriately supervised as outlined in the primary care exception requirements. As a result, services were being rendered by non-licensed residents, thus creating a variety of risks, as outlined earlier.

In the clinic, the physician examines a patient and determines that he or she has an impacted cerumen and asks the medical assistant (MA), nurse, or PA to perform an ear lavage. Is this a problem under the “incident-to” provisions for Medicare in this setting?

Depending on the carrier and the state in which the service was performed, an ear lavage is either bundled into an evaluation and management service when rendered on the same day or requires physician involvement, et cetera. In addition, some carriers have indicated that they will allow an ear lavage performed by an NP or PA but not if it is rendered by the MA or nurse under the “incident-to” provisions.

Referring to the state scope of practice, however, is critical as other requirements may apply. Some states, such as Virginia, require “direct” supervision of the PA when performing procedures. Understanding what the expectation is under “direct” supervision is essential. Medicare’s “direct” supervision requirements state that the physician does not have to be physically in the same room. However, he or she must be in the office suite and immediately available when the service is being provided. The Virginia Board of Medicine Regulations Governing the Practice of Physician Assistants defines “direct” supervision to mean that the physician is in the room in which the procedure is performed.

Now imagine what some of the potential vulnerabilities may be if an organization

CONTINUED ON PAGE 63
One Size Does Not Fit All When It Comes to Corporate Compliance and Internal Audit Organizational Reporting Structure

Several Key Standards (and Strategies) to Consider When Merging the Two Functions

Kelly Nueske

To merge or not to merge the reporting structure for compliance and internal audit — a question that can stimulate an interesting debate with no easy answer. Health care leaders ask the question frequently as they look for ways to be more efficient with diminishing resources, whether monetary or people. Another reason for asking is the perception that there is duplication of effort between the two functions. There does not seem to be a “right” answer but rather a need for thoughtful consideration when evaluating, the reporting structure for these two functions.

Internal audit and compliance have some similarities when you look at their objectives. In many health care organizations, both assist management with identifying and mitigating risks, report to senior management and the board or board committee, and maintain objectivity and independence by having no operational accountability. Maintaining independence from each other, however, is the challenge when merged under a single leader. The Institute of Internal Auditors (IIA) International Standards for the Professional Practice of Internal Auditing defines internal audit as follows:

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
The focus of the debate is around the words “independent, objective assurance.” Assurance in the internal audit world is defined as an objective assessment of an area to formulate an independent opinion on the risks and controls related to processes and systems. Ideally, to maintain this independence and instill credibility in the audit function, internal audit reports to a chief audit executive (CAE) with no other functional responsibility and access to the chief executive officer (CEO) and board or board committee. Many question whether independence can be maintained if the CAE also has accountability for the organization’s compliance function.

Separation of reporting relationships ensures that roles and responsibilities are clear, there is no co-mingling of resources, and internal audit maintains independence without question. It also helps create clear delineation between auditing and monitoring for management and the board or board committee.

Auditing should be an objective process focusing on risk and controls performed in accordance with the IIA standards, which include individual objectivity, proficiency, due professional care, and a quality assurance and improvement program. Monitoring should be an ongoing process within operations by management to validate that processes are followed to meet departmental or organizational objectives for compliance or operating performance. In the ideal situation, internal audit would complete the audits and compliance would focus on monitoring.

Even with separate reporting relationships, internal audit and compliance should work together to avoid duplication and ensure organizational effectiveness. Organizations with successful, separate functions work in collaboration to perform risk assessments, ask each other for input-related annual work plan development, and compare work plans to validate the absence of duplication. It is not uncommon for compliance to be an internal audit customer, whereby internal audit assesses the controls in an area of concern and compliance then works with management to develop corrective action plans that include monitoring activities.

The other key success factor is excellent, open communication. Sometimes it creates a positive tension resulting in a better product in the end because each area brings a different perspective when looking at risk. There are many ways to accomplish this, and in some organizations the internal audit department shares all audit findings with compliance to foster this openness and collaboration.

On the flip side, supporters of internal audit and compliance reporting to one senior manager believe there are a number of benefits. Senior managers with both functional areas indicate synergy occurs between the two areas, and there is greater influence to stimulate change within an organization when compliance and internal audit report to one senior manager. This arrangement also is believed to promote more career opportunities for staff and management. Often, performing the internal audit function is not considered operational experience, but the compliance function is considered operations. Accordingly, the knowledge and experience gained by these functional areas through working together fosters broader skill sets.

**IIA Standards and Strategies for Accomplishing Them**

If an organization wants to merge the two functional areas from a reporting perspective, the IIA standards should be addressed with a strategy developed to meet each of them without question. There are six key standards, and the following are some strategies that have been used by organizations to address them.

**Attribute Standard 1000 — Purpose, Authority, and Responsibility**

This standard states the internal audit activity should be defined in a charter, consistent with the standards and approved by the board. Both internal audit and compliance...
should have separate charters approved by the board or a board committee that clearly define their separation of duties. Typically the internal audit charter is much broader, as it focuses on controls and assurance in all areas (compliance, information systems, financial, and operational). The compliance charter typically is more narrowly focused on regulatory issues throughout the organization. There also should be a plan to deal with conflict resolution between the two functional areas that takes the chief audit executive/corporate integrity officer (CAE/CIO) out of the mix.

**Attribute Standard 1100 — Independence and Objectivity**

This standard states that the internal audit activity should be independent and the CAE should report to a level in the organization that allows the freedom to determine the scope of internal auditing, performing work, and communicating results. To achieve this, internal audit and compliance should have separate processes for risk assessment and developing individual work plans. That does not preclude the two areas from collaborating to avoid duplication prior to submitting the separate risk assessments and work plans to the board or board committee for approval.

The other key component is separate reporting on work plan progress to the board or board committee. Many CAE/CIOs have their audit manager and compliance manager present the findings and progress on the annual work plans to the board or board committee to support the independence of the two areas.

Another key to meeting the independence standard is not co-mingling resources on projects. Internal audit needs to focus on conducting assurance and consulting activities in accordance with the standards. Compliance needs to focus on day-to-day operations, such as the integrity hot line, training, policy development, investigations, corrective action plans, and monitoring activities. Co-mingling the resources for these activities will jeopardize the independence and credibility of the internal audit function.

**Attribute Standard 1130 — Impairments to Independence or Objectivity; and Attribute Standard 1300 — Quality Assurance and Improvement Program**

These standards state the following:
- If independence or objectivity is impaired in fact or appearance, the details should be disclosed to appropriate parties.
- Objectivity is presumed impaired if the auditor provides assurance services for an area for which he or she had responsibility in the past year.
- Assurance engagements for functions for which the CAE has responsibility should be overseen by an outside party.
- Internal audit should adopt a process to monitor overall effectiveness that should include internal and external assessments.
- External assessments of internal audit should be conducted at least every five years by a qualified, independent reviewer or review team outside the organization.

The best way to meet these standards is to have both areas reviewed by external resources. Some CAE/CIOs assess compliance program effectiveness every year or two using external resources for the engagement depending on the risks. In addition, it is important to have a quality assurance review conducted for the internal audit processes in accordance with the standards every five years. The IIA outlines two different methods to meet this standard. Both areas should have the results reported to the board or board committee once completed.

**Attribute Standard 1200 — Proficiency and Due Professional Care; and Attribute Standard 1210 — Proficiency**

These standards state that an organization’s internal auditors collectively should possess the knowledge, skills, or competencies to perform their responsi-
bilities, and the CAE should obtain competent advice and assistance if knowledge, skills, or competencies are lacking. If one applies these expectations to the CAE, it might be difficult to recruit a CAE/CIO with strong knowledge, skills, and experience in both internal audit and compliance. This can be addressed, however, through management and staffing of the functional areas.

If the CAE/CIO has a compliance or legal background, the internal audit activities should be managed by an audit manager with a strong background in financial, information systems, and operational audit experience to fill any gaps in senior management experience. In contrast, if the CAE/CIO has an internal audit background, compliance activities should be managed by a compliance manager with a strong compliance or legal background. The key is filling the gaps with management and staff that have strong experience in the functional areas.

Performance Standard 2000 — Managing the Internal Audit Activity; and Performance Standard 2050 — Coordination

These standards state that the CAE should effectively manage internal audit to ensure it adds value to the organization, and information should be shared to coordinate activities to ensure proper coverage and minimize duplication. Some would say these standards indicate a single reporting relationship is acceptable. The key, however, is that there is sharing and collaboration, but the two areas should not be influenced in their activities by the other.

Again, keeping separate risk assessment and work plan development processes is essential with periodic, separate reporting to the board or board committee on the findings and activities. If the internal audit function identifies a risk area for which the compliance area is responsible, it should be included in the work plan and assessed in the same manner as any other risk area.

Performance Standard 2120 — Control

This standard states that internal audit should assist the organization in maintaining effective controls by evaluating their effectiveness and efficiency and promoting continuous improvement. Internal audit should ascertain the extent to which controls and operating results are consistent with the organization's goals and objectives as they relate to governance, operations, and information systems.

If internal audit identifies findings related to a compliance area, the compliance function can work with management to implement the appropriate changes and monitor the corrective action plans. Clarity for these responsibilities should be outlined in the charters for each area, and it should be clear to an outside reviewer that the activities are separate and independent of each other.

Conclusion

Ideally, the reporting relationship for internal audit and compliance would be separate. If an organization wants to pursue a single reporting relationship, however, a thoughtful, disciplined, and transparent approach to the decision and implementation that is clearly communicated throughout the organization is recommended. It may save money initially to have one senior manager over the two functions, but the savings may become difficult to quantify over time if additional controls need to be implemented or additional staff is needed to support the two functions operating independently.

It isn't necessary to move to a single reporting relationship to accomplish synergy and collaboration. The same result may also be accomplished with strong, collaborative leaders over the functional areas. In the end, it really depends on the culture of the organization; one size does not fit all.
Kimberly Brandt Discusses the Program Effectiveness Project, Medicare and Medicaid Risk Areas, and Helpful Resources

Kimberly Brandt is the director of the Program Integrity Group for the Centers for Medicare and Medicaid Services (CMS). Prior to joining the Program Integrity Group, Ms. Brandt worked for more than five years with the Office of Inspector General (OIG) in a variety of progressively challenging jobs: as senior counsel in the OIG’s Office of Counsel; special counsel for External Affairs; and director of External Affairs.

In this interview, Ms. Brandt discusses the compliance program effectiveness project she is working on currently and provides insight on key issues such as Medicaid, Medicare, and credentialing.

**Snell:** Please tell us a little about your background.

**Brandt:** I have been director of Program Integrity at CMS since February 2004. Before that, I worked for the OIG in the Office of Counsel and in the immediate office of the Inspector General for a total of five years. My undergraduate training is in political science, but after college I worked on Capitol Hill for three years as a health care staffer for a member of Congress and the House Energy and Commerce Committee.

That experience helped spark my interest in health care issues, particularly Medicare and Medicaid, so I went on to get a law degree with a concentration in health law from DePaul College of Law in Chicago. I have never regretted that decision; in my almost nine years working for the federal government, there has never been a day when I have been bored.
Snell: Please tell us about the compliance program effectiveness project you are working on and what you have learned from the project.

Brandt: The CMS compliance effectiveness program is coming to completion after three years. We started the project to assess whether an entity having a compliance program made any sort of appreciable difference in the accuracy of its Medicare claims submissions. Sixteen hospitals from the northeast region of the country have participated in the pilot, and it has been a very beneficial undertaking for both the participants and CMS.

While the final results will be released later this spring, the biggest lesson learned from the project is that we were able to show that certain aspects of a compliance program do make a difference on the accuracy of an entity's claims submissions. It was very interesting for CMS and the pilot participants to see which elements had the biggest impact as well as the unique features of how that element as implemented in an entity's compliance program made a positive or negative impact.

Additional lessons learned were that the compliance officer's interactions with people throughout an entity made a big impact on the effectiveness of the program, as did the level of buy in from the board or governing body. In other words, if compliance was not seen as part of the overall culture at the entity, there did seem to be a correlative impact on the accuracy of the entity's billings.

Snell: There seems to have been an increased amount of activity in Medicaid enforcement at the state level. Please tell us about this activity and how it may affect providers.

Brandt: The Deficit Reduction Act of 2006 included language mandating an increased focus on Medicaid fraud and abuse activities at both the state and federal level. As such, providers will be seeing an increasing focus on Medicaid billings as these provisions are implemented.

Traditionally, most providers have mainly concentrated on Medicare billings. The message now is that providers should pay equal attention to Medicaid. CMS has created an entire new Medicaid Integrity Group, which will focus on not only finding areas of fraud and abuse at the provider level in Medicaid but also working with states to improve and enhance their state program integrity efforts.

Snell: Currently, what are the most important risk areas in Medicaid compliance?

Brandt: I do not have any particular ones that stand out right now. CMS, however, is currently in the process of compiling the data from the first year of its PERM (Medicaid error rate) program. That program is collecting a statistically valid sample of Medicaid fee-for-service claims from 17 states for fiscal year 2006 and will be reporting the results of that claims review by the end of calendar year 2007. Going forward, PERM will be measuring Medicaid fee-for-service, SCHIP, and eligibility claims accuracy for 17 states each year. Ultimately, the results of the PERM project can be used as a diagnostic tool for both provider and service-specific error rates.

Snell: Currently, what are the most important risk areas in Medicare compliance?

Brandt: The most important risk areas in Medicare compliance are medical necessity, meeting and continued compliance with Medicare enrollment standards, and lack of appropriate medical documentation.

Snell: What should compliance professionals be looking out for in the area of credentialing of caregivers? It seems there is stepped-up enforcement of regulations that require that a provider have a particular credential to legally bill for a particular service.

Brandt: Compliance professionals should evaluate education, competency, licens-
The two key national movements involving e-health and quality of care should be on every compliance officer’s radar screen. These two areas of focus not only are related but also should present a new emphasis and perspective in your compliance programs in the years to come. The move to transparency in cost and pricing of health care services as well as increased reporting of quality measures will become a driving indicator of compliance, too.

**Health Information Technology**

According to the e-health initiatives budget analysis, President Bush’s proposed 2008 federal budget includes allocating $118 million for the Health and Human Services’ Office of the National Coordinator for Health Information Technology (ONC). The link between health information technology (HIT) and better quality health care continues to be a key highlighted component of the President’s spending request, along with the following:

- Health care affordability and consumer control;
- Increasing health insurance access and ensuring that all citizens have access to basic coverage at an affordable rate;
- Utilizing information technology to move toward personalized medicine, linking critical care with research to improve health care quality;
- Strengthening Medicare’s sustainability;
- Improving community health centers;
- Continued Medicaid transformation and state/federal program cooperation;
- State Children’s Health Insurance Program re-authorization and funding increases;
- Addressing HIV/AIDS;

**Web Sites Offer Information on Federal, State, and Organizational Efforts to Improve Health Care**

ELECTRONIC RESOURCES

Catherine M. Boerner, JD, is the president of Boerner Consulting, LLC. She can be reached at 414/427-8263 or by email at cboerner@boernerconsultingllc.com.
Strengthening pandemic preparedness and biodefense; and

Promoting tax code and other changes that promote insurance coverage.

To learn more about the HIT initiatives, visit www.hhs.gov/healthit. On this Web site you can get information on activities around privacy and security of electronic personal health information as well. By clicking on the “Privacy and Security” link in the left column, you can then review HHS initiatives for state- and organizational-level collaboration and HHS federal activities.


STATE E-HEALTH INITIATIVES

Many states are in various stages of working on plans to adopt and exchange electronic health records. According to the e-health initiative, 12 executive orders were issued by U.S. governors calling for health information technology and health information exchange to improve health and health care. These states include:

- Arizona (2005);
- California (2006);
- Florida (2004);
- Georgia (2006);
- Illinois (2006);
- Kansas 2004);
- Missouri (2006);
- North Carolina (1994);
- Tennessee (2006);
- Texas (2006);
- Virginia (2006); and

BRIDGES TO EXCELLENCE

Another Web site to visit is the Bridges to Excellence (BTE) Web site at www.bridgestoexcellence.org. Here you can learn more about a group of employers, physicians, health plans, and patients that have come together to create “Bridges to Excellence.” The Web site explains that BTE’s purpose is to create programs that will realign everyone’s incentives around higher quality. They are guided by these three principles:

- Reengineering care processes to reduce mistakes will require investments, for which purchasers should create incentives.
- Significant reductions in defects (misuse, underuse, overuse) will reduce the waste and inefficiencies in the health care system today.
- Increased accountability and quality improvements will be encouraged by the release of comparative provider performance data, delivered to consumers in a compelling way.

BTE is a not-for-profit organization created to encourage significant leaps in the quality of care by recognizing and rewarding health care providers who demonstrate that they deliver Safe, Timely, Effective, Efficient, Equitable, and Patient-centered (STEEP) care.
The Number of Online Personal Health Records Is Growing, but Is the Data in These Records Adequately Protected?

Several Key Issues that Covered Entities Should Consider When It Comes to Personal Health Information

Personal health records (PHRs) are becoming increasingly popular among consumers. PHRs are designed to help consumers record, store, and transmit their medical information to any doctor or hospital, as well as for online health risk assessments and individual wellness program planning.

The first large-scale, online personal health record service was started in 1999 by WebMD. Since then a number of other companies have begun to offer online PHRs, including FollowMe, Laxor, and Medem. Some of these PHRs are designed not only to store information entered into the record by the individual him or herself but also to incorporate information provided directly from physician practices, hospitals, labs, and other sources of medical information. PHRs currently are offered by physician practices, hospitals, health insurers, drug companies, employers, and a variety of other public, private, and non-profit organizations.

PHRs are different from EMRs (electronic medical records). EMRs are typically implemented by health care entities as electronic repositories of clinical information generated by clinicians in the course of treating and caring for patients of the entity. Access to the EMR is usually restricted to the doctors, nurses, and other members of the workforce of the health care entity that owns the system.

Although many EMRs are Web enabled, it is usually not the vehicle by which protected health information (PHI) is shared with providers from other health care organizations or with patients. Virtually all of the organizations implementing EMRs are health care providers covered by the...
Health Insurance Portability and Accountability Act of 1996 (HIPAA) rules. Many PHRs, on the other hand, are provided by companies that are not covered entities under HIPAA and consequently are not required to comply with the HIPAA rules directly.

In addition, most PHRs contain information supplied by the individual and do not contain personal health information provided directly by covered entities; consequently, the HIPAA rules governing disclosure of PHI do not come into play. Regardless of the source of the information, however, PHRs may contain sensitive personal health information on medical conditions and histories, medications, lifestyles, et cetera, that most would agree should be protected from unauthorized access, disclosure, or use by comprehensive privacy and security policies and procedures.

The Altarum Institute recently released a report commissioned by the Office of the National Coordinator for Health Information Technology to examine the privacy policies and procedures of 30 currently available PHRs operated by organizations that are not covered by the HIPAA rules. Their findings indicated a wide disparity in the protections offered by these privacy policies with significant deficiencies in many instances. Here is a quote from the summary and recommendations section of the report:

Our review of 30 publicly available privacy policies revealed wide variation in understanding and implementation. We also note that not every PHR vendor Web site has a publicly available privacy policy, and we found more than one instance of privacy policies that could only be reached after enrolling and providing private information such as an email address.

We draw the following conclusions from our analysis:

- Consensus requirements for the contents of a PHR privacy policy do not yet exist, and many vendors appear to have focused instead on security procedures and Internet privacy descriptions;
- Transparency of secondary use of data could be greatly improved;
- The majority of vendors reviewed did not reference HIPAA;
- Data disposal rules and regulations are ill-defined, especially for closed accounts and vendors that go out of business; and
- Many specific terms including ‘personal health information’ are not defined in the privacy policy or related documentation.

A copy of the full report may be downloaded from www.hhs.gov/healthit/ahic/materials/01_07/ce/PrivacyReview.pdf.

In June 2006, the National Committee on Vital and Health Statistics (NCVHS, which advises HHS on privacy and security issues) recommended in a report sent to HHS entitled “Privacy and Confidentiality in the Nationwide Health Information Network” (NHIN) that PHRs, as part of a NHIN, be afforded strong privacy and security protections, regardless of whether or not they are operated by entities covered by HIPAA. NCVHS specifically recommended the following:

HHS should harmonize the rules governing the NHIN with the HIPAA Privacy Rule, as well as other relevant federal regulations, including those regulating substance abuse treatment records.

The full NCVHS report is available at: http://ncvhs.hhs.gov/060622lt.htm.

INTERFACES FROM EMRS TO PHRS

Some EMR companies have been partnering with PHR vendors to interface an EMR directly to a PHR. These interfaces take a
Compliance Teams — Are They a Good Thing?

One Example of How Compliance Teams May Be Structured and What They May Be Asked to Do

Are compliance teams a good thing? What are they? How do they work? Do they help or hinder the process of compliance? Are they a fad or a trend?

At the organization where I work (which is an integrated health system), compliance teams have been incorporated into the compliance program. This was done to address compliance risk and concern in each of the integrated health system’s entities. Each entity has similar and unique risk areas and issues.

The compliance teams develop and propagate compliance standards and protocols. They assist in overseeing the operation of the compliance program. The teams include hospital, medical group, durable medical equipment (DME) company, home health, ambulance, and business research representatives. More specifically, the team members include the following:

Hospital — Revenue management executive partner, hospital business office representative, hospital admitting representative, information technology representative, utilization review manager, chief financial officer, hospital reimbursement representative, billing compliance manager, billing compliance analyst, hospital coding manager, chief of staff of medical executive committee, executive partner of reimbursement and contracting.

Medical Group — Physician representative, executive partner, revenue management services, pharmacy representative, laboratory representative, billing compliance manager, billing compliance analyst, medical group coding and reimbursement manager, clinic insurance manager, patient services admitting manager, executive partner reimbursement and contracting, chief of staff of medical executive committee, chief financial officer.
DME Company — Corporate compliance coordinator of the DME, billing compliance manager, DME reimbursement manager.

Home Health — Home health manager, billing compliance manager, home health operations manager, home health clinical coordinator, billing compliance analyst.

Ambulance — Ambulance executive director, billing compliance manager, ambulance education coordinator, ambulance business officer, ambulance clinical coordinator, billing compliance analyst.

Business Research — Chief financial officer, billing compliance manager, hospital reimbursement manager, budget coordinator, accounting coordinator, billing compliance analyst, physician senior executive, pharmacy representative, research coordinators, federal research business analyst, health information management representative, and clinical research site manager.

Duties of the compliance teams include the following:

- Receive and act upon reports and recommendations from the billing compliance manager, which are generated by the system’s program to monitor and review compliance.
- Maintain a record of the items discussed and actions taken at each meeting of the compliance team.
- Serve at the billing compliance manager’s discretion on subcommittees to address specified issues.
- Perform other functions that may be reasonably necessary to fulfill the compliance team's responsibilities and purpose.
- Regularly attend the scheduled and additionally called meetings of the compliance teams. (Absence may be excused by the billing compliance manager for good cause.)
- Maintain confidentiality of any and all sensitive information regarding individuals or the health system.
- Provide input to policy development and process implementation.
- Provide risk assessment, which includes annual Office of Inspector General work plan evaluation and action.

Designated associates are asked to participate as needed based upon individual issues.

Each compliance team works to achieve consensus. If consensus cannot be reached, a summary of the issue is sent to the Compliance and Internal Audit Steering Committee for a final decision. This committee is made up of high-level senior executives.

The hospital and medical group teams meet every other month. The other teams meet quarterly or more often if necessary. The teams are chaired by the billing compliance manager. Minutes of the meeting are kept, reviewed and approved by the team members. These teams have proven to be a valuable part of the compliance program to assist in evaluating risk areas, assigning accountability, and follow up.
President Bush’s Proposed Budget for FY 2008: Trying to Balance Expense and Need in the Health Care System

An Overview of the Administration’s Proposals for Change to the Health Care System

President Bush released his proposed budget for fiscal year (FY) 2008 on February 5, 2007. As might be expected, the Bush Administration’s goals for the proposed budget include permanent tax relief and other “pro-growth” policies. The proposed budget also addresses several key areas of health care reform, including the following:

- Providing health services to underserved populations through state and federal programs;
- Strengthening Medicare and Medicaid’s long-term financial security by reducing expenses; and
- Modernizing the Medicare system through quality improvement and reallocation of funds.¹

It is clear that the proposed budget will have significant financial impact on hospitals, physicians, and the provision of health care services generally. Below is an overview of the Administration’s health care proposals.

EMPLOYER-SPONSORED INSURANCE

Currently, only employer-sponsored insurance costs qualify for a deduction on federal tax returns. The proposed budget, however, would change this by permitting individuals and families who obtain, at a minimum, catastrophic health insurance to receive a deduction as well. Specifically, the proposal sets forth a framework in which individuals receive a $7,500 deduction and families receive a $15,000 deduction.²

SUBSIDY OF THE UNINSURED

It is well accepted that the use of emergency rooms as a primary source of care substantially increases the cost of
health care — a serious problem facing all communities. The Administration proposes to create a health care system whereby a portion of institutional payments would be reallocated to subsidize the purchase of private health insurance for people with “limited income.”

The thought behind this redirection is that if all Americans are insured, and have access to primary care, the high costs of emergency care could be reduced. No clear guidance, however, is provided as to how this is to be accomplished. Moreover, the responsibility for the creation and administration of such a program is delegated to the states.3

**SLOW THE GROWTH OF SPENDING**

Anticipating that “by 2030 projected spending for Medicare, Medicaid, and Social Security will be almost 60 percent of the entire Federal budget” and that Medicare Part A will reach insolvency by 2018,4 the proposed budget seeks to slow the growth rate of health care entitlement plans — Medicare and Medicaid.

**MEDICARE**

The Administration’s primary strategy to achieve more sustainable health care expenditures over the next five years involves reductions in most providers’ fee schedules, including inpatient hospitals, outpatient hospitals, hospices, and ambulance services; skilled nursing facilities and inpatient rehabilitation facilities; home health agencies; and ambulatory surgical centers. Additional legislative and administrative cuts are expected.5

**MEDICAID**

The Administration plans to reauthorize the State Children’s Health Insurance Program and to allot to it an additional five billion dollars and raise payments to end stage renal disease facilities by 1.6 percent beginning in April 2007.6 Medicaid, however, will see a decreased rate of growth, primarily through administrative reform.

The bulk of the administrative reform will be accomplished by (1) phasing out payment for some services, such as transportation and some Medicaid services provided in schools; (2) eliminating Medicaid payments for graduate medical education; and (3) clarifying the definition of rehabilitation services that may be billed under Medicaid.7

**REALLOCATION OF FUNDS**

One objective of the proposed budget is to ensure that people with genuine financial need are given appropriate funding. Funds will be provided to the Indian Health Service, HIV/AIDS patients and testing programs, and first responders at the World Trade Center — all identified by the Administration as populations in need.8 Another objective is to continue to protect the overall health of the nation.

To this end, funds will be given to (1) protect the nation against bioterrorism and an influenza pandemic; (2) fund almost 10,200 new and competing medical research grants; (3) aid those trying to overcome substance abuse; and (4) supplement the income of caretakers who choose to care for their elderly family members in their homes.9

**QUALITY IMPROVEMENT**

Some of the strategies to improve health care do not involve strictly financial maneuvering. CMS is in the process of making plans to implement new quality reporting measures for physicians, outpatient centers, and ambulatory surgical centers. They are working to rationalize payments and to reduce the number of erroneous Medicare payments.10

The proposed budget has garnered criticism and skepticism from a variety of interested parties. Providers, understandably, are dismayed by reduced fees. Typically, private insurance companies base their fee schedules on federal rates, so a reduction in Medicare payment rates may result in a reduction in payment rates not only to federal beneficiaries, but also from commercial payors. Thus, providers worry that these reduced rates may prevent them

CONTINUED ON PAGE 66
Physicians and Other Providers Interested in EHR
Should Contact the QIO in Their State

CMS is funding the quality improvement organizations (QIOs) in each state to assist primary care physician offices in improving access to patient information, decision support, and reference data, as well as enhance patient-physician communication, thereby improving the quality and safety of care given to Medicare beneficiaries.

A key component of these efforts is the Doctor's Office Quality Information Technology (DOQ-IT) project — a three-year, national quality improvement initiative offering help to physicians who wish to purchase, implement, and fully utilize electronic health records (EHRs) in their practices.

DOQ-IT’s overarching purpose is information technology infrastructure development. The QIOs provide participating physicians with free assistance in selecting, implementing, and optimizing IT systems such as EHRs, e-prescribing, and registries. Recruitment began in July 2005; today, the DOQ-IT identified participant group (IPG) includes approximately 5 percent of adult primary care practices nationwide. Although enrollment in each of the QIO IPGs is now closed, interested physicians should check with their state’s QIO for Web-based DOQ-IT materials that they would like to use.

GOALS AND OBJECTIVES OF THE DOQ-IT PROJECT

The objectives of DOQ-IT are to promote the production and effective use of electronic clinical information necessary for improving clinical performance; office practice process redesign that includes care management and self management of patients with chronic conditions and preventive services needs; and voluntary quality performance data submission using an existing set of clinical performance measures to a single protected all-payer data warehouse.

Harry M. Feder, MPA, is the senior vice president of IPRO, the QIO for the State of New York. Mr. Feder is responsible for the monitoring and assessment of health care provided to Medicare, Medicaid, and private patients across the continuum of care. He can be reached at 516/326-7767, ext. 528, or by email at hfeder@ipro.org.

This material was prepared by IPRO, the Medicare Quality Improvement Organization for New York State, under contract with the Centers for Medicare and Medicaid Services (CMS), an agency of the U.S. Department of Health and Human Services. The contents do not necessarily reflect CMS policy. (850W-NY-TSK1D1-07-01)
Longer-term goals include helping physicians improve access to patient information, decision support, and reference data, as well as enhancing patient-physician communication, thereby improving the quality and safety of care given to all patients, including Medicare beneficiaries.

**Clinical Areas**
Clinical measures that are being used to track progress and improvement in the DOQ-IT project include coronary artery disease; diabetes mellitus; heart failure; hypertension; and preventive care. The clinical metrics are based, in part, upon the American Medical Association Physician Consortium for Performance Improvement measures. There is no threshold for adherence to the measures. A participating practice can choose which measures it will submit, and submission is not mandatory for DOQ-IT involvement.

Ultimately, DOQ-IT participating practices will report their performance on the selected measures via a standardized EHR platform to a QIO clinical warehouse. The QIO clinical warehouse will receive, review, and validate electronically transmitted information regarding practitioner performance and identify opportunities for improvement.

**Project Process and Requirements**
Individual QIO approaches may vary; however, they are based on principles of change management and accumulated experience from hundreds of small-to-medium sized practices that have made the move to an EHR system. QIOs work with practices throughout the process, acting as an extension of practice teams. They help to assess EHR readiness; educate on EHR functionality requirements and vendor selection; provide guidance on EHR implementation planning, including office workflow redesign; and advise on interoperability considerations and the use of EHRs for care management and quality improvement.

QIOs provide vendor-neutral information on available technology solutions and help practices to determine the best system for their offices. The vendors chosen by each practice are responsible for installing the EHR system, providing training to staff, and maintaining technical support services. Although DOQ-IT does not provide capital funding for implementation, QIOs are working in conjunction with national and state initiatives that provide financial incentives to practices that commit to redesigns that include expanded information technology solutions.

**Benefits of DOQ-IT Participation**
- Investigate EHR features, functionality, and purchasing options.
- Receive objective information from experts about EHR selection, price negotiation, and implementation.
- Analyze individual practice needs and readiness to adopt an EHR system.
- Optimize the use of an EHR system, and effectively overcome challenges associated with implementation.
- Assess current practice workflow and craft revised strategies to create efficiencies and capitalize on the opportunities offered by an EHR system.
- Obtain valuable insight and support from peers engaged in EHR implementation.
- Receive complementary support (Web-based conferences, onsite visits) in addition to that provided by the EHR vendor. Physicians and other providers interested in EHR should contact the QIO in their state. A complete directory of QIOs by state appears online at http://www.medqic.org.
The role of the compliance officer is now well established in many health care organizations, yet many compliance activities have been restricted to liabilities associated with false claims, upcoding, and other billing transgressions. Further, many compliance officers and their staff operate in some ways parallel to but apart from the fundamental activities of the health care enterprises they serve. Because of concerns about the independence of the compliance function, compliance can find itself isolated from the strategic and operational center of the organization.

No matter the internal view of where the center lies, every sector of the health care industry — whether hospital, physician practice, medical device manufacturer, billing company, imaging center, or nursing home — has as its ultimate obligation and purpose to contribute to clinical processes of care for patients; whether to cure them, heal them, or palliate them. Today, the strategic mission of any health care enterprise is to provide optimal quality of care to patients, the ultimate beneficiaries of their raison d'être.

Parallel with the maturation of the compliance industry, demands to demonstrate that health care enterprises are providing optimal quality of care can be seen in the multiplying statutory, contractual, regulatory, and market-based programs mandating transparency, pay-for-performance, reported sentinel events, and more. Few people, however, are aware that every single model compliance guidance from the Office of Inspector General (OIG) also makes reference to quality. In addition, beginning in 2002, every one of the OIG’s work plans has included a reference to quality.

From the perspective of the Department of Justice, the new quality era began with the Tucker House case in

**Several Suggestions for How to Effectively Integrate Quality-Oriented Issues into Workflow**
which the facility paid $535,000 and agreed to apply clinical practice guidelines for the treatment of bedsores when the government charged the facility with false claims for every day of care it had been paid for patients who had developed aggravated decubiti. The theory of the case turned on the fact that one of the contributing factors in bad bed sores is malnutrition; therefore, each claim by the facility for a day of payment was false since the facility implicitly did not feed the patients effectively. The theory was further applied throughout the country in more than 40 additional settlements, often instigated by whistleblowers.

In 2003, a hospital in Michigan pled guilty to criminal charges and paid a $1.05 million fine when a prolific anesthesiologist on staff performed unnecessary pain management procedures for which the hospital was paid the associated facility fees. Patients suffered significant complications from the unnecessary surgeries around which false claims arguments were fashioned. Similarly, the unnecessary surgery at the Tenet Hospital in Redding, California, led to the sale of the hospital in response to prosecutorial initiatives.

Against this flourishing background, it is noteworthy that James G. Sheehan, associate attorney in the U.S. Attorney's Office in Philadelphia, has now targeted quality in even more innovative ways. With the advent of pay-for-performance programs in Medicare, both for hospitals and physicians, Sheehan has made it abundantly clear that his offices will be interested in “the quality we are paying for.” He has stated that he is interested in seeing the reduction of medical errors and adverse events; improvement in actual clinical outcomes; compliance with clinical practice guidelines or other clinical requirements; and reduction in cost of care for the same outcomes.

The core question around which fraud enforcement will focus in the quality arena is conduct by an institution which perpetuates care of less than optimal quality. Sheehan's attention is directed to gross and systemic leadership failures where there has been notice, warning, and failure to act; intentional acts by individuals; false reporting or failure to report quality-relevant failures; “appalling outcomes;” and more.

Although these new prosecutorial initiatives may be startling, readers should note that there are longstanding bases for exclusion from Medicare based on quality failures. When an entity provides items or services to patients (whether or not eligible for benefits under Medicare or Medicaid) that are substantially in excess of the patient's needs or of a quality that fails to meet professionally recognized standards of care, there is no need for a criminal prosecution nor recovery of enormous false claims dollars to bar the provider from Medicare.

On the other hand, there are also significant civil money penalties to be imposed for quality failures. Examples include claims for a pattern of medical items or services that a person knows or should know are not medically necessary; provision of false or misleading information that could be expected to lead to a premature discharge; and hospital payments to physicians to reduce services — the provision which inhibits gain sharing except in very narrow circumstances.

All tolled, it is hard to imagine how compliance officers can claim to be doing their job if they are not fully integrated in the quality improvement activities of their organizations — and particularly in hospitals and physician enterprises. In terms of where clinical standards of behavior are emerging, the activities of the Institute for Healthcare Improvement (IHI) are expanding and defining a new world. Beginning with “The 100,000 Lives Campaign” through which more than 3,000 hospitals holding 80 percent of the beds in the United States pledged to deliver six specific combinations of services to reduce needless deaths, the clinical standard of care was changed overnight.

CONTINUED ON PAGE 66
You May Want to Revisit (and Reevaluate) Your Annual Risk Work Plan

Six Important Questions You Probably Need to Ask Yourself

Although you may have developed your annual risk work plan, which outlines the specific areas in which you plan to conduct auditing and monitoring, you may want to modify your original approach. For example, let’s assume you indicated you were going to conduct audits in your behavioral health department.

The first thing you should do is prepare and document your approach. This step includes development of your testing criteria based on rules and regulations. The next step is defining the data attributes that are going to be validated prior to beginning. There are many questions that need to be confirmed such as:

WHO ARE THE CARE PROVIDERS RENDERING SERVICE IN THE SPECIFIC AREA?

There are a variety of clinicians who can be involved in patient care within behavioral health, including:
- Licensed clinical social workers (LCSW);
- Clinical psychologists;
- Psychiatrists; and
- Counselors.

It is important to understand each practitioner’s state scope of practice as well as what they can or cannot code for billing purposes.

WHERE ARE THE SERVICES RENDERED?

Behavioral health services, such as the following, can be rendered across various settings within an organization:
- Office (POS 11);
- Inpatient hospital (POS 21);
- Outpatient hospital (POS 22);
- Community mental health clinic (POS 53); and
- Partial hospitalization (POS 52).
Knowing the location where the service took place will help you decide where your risks are. If you use nonphysician providers in the inpatient or outpatient hospital setting, you will want to make sure you are reporting their services correctly. Remember that “incident to” is only allowed in an office setting (POS 11). You cannot report services as “incident to” in any other setting.

**WHAT ARE THE SPECIFIC PAYER REQUIREMENTS?**

Understanding the payer mix is important to access what your patient population looks like. Even though most organizations apply either Medicare or Medicaid regulations when conducting their audits, there may be “other” specific contractual requirements that need to be considered.

**DO YOU USE AN OUTSIDE BILLING AGENCY?**

If you use an outside billing agency, you should consider including in your audit a comparison of the practitioner encounter form, the CMS-1500 form, and the payer’s explanation of benefits (EOB) form. This should be done to ensure that the information reported was accurate from start to end.

Analyzing the documentation from start to end can help identify problems encountered during the billing process. You may identify risk areas, such as services incorrectly reported as “incident-to” or services that had been reported with the incorrect place of service code.

**WHAT ARE THE HIGH-RISK AREAS FOR BEHAVIORAL HEALTH?**

You may want to start with the Office of Inspector General (OIG) work plan to determine high-risk areas for behavioral health. This year there are a number of areas identified for psychiatric facilities and providers. There is one area, however, that is specifically focused on Medicare Part B professional services: psychiatric services in an inpatient setting.

The focus of this work plan initiative is to ensure that practitioners have not reported inpatient group therapy services as individual therapy services. Because individual therapy services are reimbursed at a higher rate than group therapy, the OIG believes this could lead to inappropriate reporting.1

**WHAT IS THE NUMBER OF SERVICES REPORTED PER PROVIDER?**

Another risk area for behavioral health is reporting more services than are possible on a given day. Because many of the behavioral health services are based on time, you need to monitor how many hours or services your providers report on a specific date of service. You can accomplish this by randomly pulling data for a specific practitioner on a specific date of service.

Next, compare this data with the practitioner's billing data. For example, if a practitioner sees 13 patients per day and reports 45 to 50 minutes of outpatient psychotherapy per patient, this could be considered high. On the other hand, if the practitioner had seen 13 patients and reported 20 to 25 minutes of outpatient psychotherapy per patient, this would be reasonable.

There have been some providers who have reported more services than they could provide in a 24-hour period and have been investigated by the government. One recent case involved a psychiatrist who reported services for more than 116 patients in a single day. The psychiatrist settled for a repayment of $216,000.2

In addition, you should be mindful of potential statistical analysis your payer may be using. One Medicare Health Care Integrity Team used a statistical tool to detect the number of hours of service providers billed in a 24-hour period. The team identified providers billing 36 hours of service in a 24-hour period. Further, they indicated that providers who bill more than 9.67 hours of service in a 24-hour period may be considered aberrant and may be reviewed by Medicare.3

CONTINUED ON PAGE 67
AHIMA Report Addresses Evolving Role of Health Care Privacy and Security Officers

Expanded Role of IT Requires Health Care Professionals to Reevaluate How They Do Business

Those who are new to compliance may still be trying to figure out what their roles are and how exactly to decipher and apply the myriad federal and state regulations, but that does not mean those who have been in compliance for a while have it all figured out and can just sit back and take it easy. Compliance is an ever-changing profession, and nowhere is that more evident than when it comes to privacy and security.

In light of new privacy-related issues, including the evolution of health information exchanges, state-level privacy and security standards that are more stringent than the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and numerous high-profile security and privacy breaches, the role of privacy officers in health care has evolved over the past four years, according to a report issued recently by the American Health Information Management Association (AHIMA).

The report, “On the Front Lines of Healthcare Privacy,” released in conjunction with Health Information Privacy and Security Week (April 8 – 14, 2007), looks at the changing privacy and security landscape as well as the role of the privacy officer. In the report, AHIMA spoke with four privacy professionals, all of whom provide insight on how privacy officers:

- Now play a broader role than ever before within their health care organizations;
- Do work that has become more complex with the introduction of health information exchange and increased interest from the public;
- Face challenges that still exist with some HIPAA standards; and
- Deal with the long-standing task of educating consumers about their privacy rights.
This article examines each of these items a little more closely and offers insight on the challenges inherent with change and how to train appropriately in the face of those changes.

**Expanded Role of Privacy and Security Officers**
The role of health care privacy and security officials is as dynamic as the industry itself. Their responsibilities are stretching as the industry stretches. Privacy and security officials are being sought out for their expertise in confidential practices in policy setting and troubleshooting regardless of whether the involved data is protected health information (PHI) or another type of confidential information, such as proprietary or business assets. Their expertise is applicable and transferable to support organizational concerns in ways not originally carved out by the HIPAA privacy and security rules.

**Advances in Technology**
The roles of these officials are becoming more complex with technology advances and industry initiatives, such as the electronic health record (EHR), the personal health record (PHR), and health information exchange (HIE). Organization privacy and security programs must keep pace and integrate with any future changes, such as standards setting, best practices development, and changing laws and regulations.

Officials need knowledge of more laws and regulations and need to work closely with individuals (such as corporate counsel and corporate compliance, risk management, and human resources personnel) in situations in which responsibilities intersect and overlap — and they are working more directly with the public. There is a need for positional authority within their organizations to accompany expanding responsibilities.

**Existing Challenges with Some HIPAA Standards**
Health care has work to do to address consumer education needs. The world of privacy is complicated even to the health care worker. Widely publicized security incidents add to consumer concerns.

The industry has an ongoing challenge to simplify the message for consumers to reduce misunderstanding or misinterpretation and ensure they understand how to exercise their privacy rights. At the organizational level, staff knowledge through training is critical for this, especially in the frontlines where patients are encountered. Well-trained staff can answer questions, guide consumers in their privacy rights, and ensure assistance from privacy leadership when interpretation is difficult.

**Long-Standing Task of Education**
The health care industry faces an HIE challenge due to laws and regulations differences, both within a state and as they coexist with HIPAA. Issues are made even more complex when consideration is given to information flow that crosses state lines. Health care professionals need to find a way to integrate laws with the mission of improving quality of care and patient safety that is respectful of health care ethics.

**Challenges Inherent with Changes**
It is important to note that information technology is requiring health care professionals to reevaluate how they do just about everything information related. Transitioning to an electronic environment, even in degrees, calls for operational redesign and new approaches to handling PHI in a confidential manner. Some paper privacy and security issues are being cancelled out and replaced by new challenges brought on by technology.

HIPAA helped move privacy and security into the national limelight. The privacy rule established minimum levels by creating a privacy floor. Security practices well established in other industries became requirements for covered entities within health care.

There is no question the industry goal of HIE requires major stakeholder collaboration for exchange success. We have come to

CONTINUED ON PAGE 67
Should Your Hot Line Be Outsourced, or Should it Be Operated in House?

Several Factors to Consider When It Comes to Making This Decision

One thing is clear when it comes to hot lines: companies must establish and publicize a system through which employees and agents can report improper or criminal conduct within the organization without fear of retribution. This article offers several tips that are designed to assist compliance officers in making the decision whether to operate their hot line internally or outsource it.

The U.S. Sentencing Commission guidelines call for the “establishment of a systematic approach for employees to report violations outside the chain of command to a higher authority in the company.” The Office of Inspector General’s (OIG’s) Compliance Program Guidance for Hospitals states that “the OIG encourages the use of hot lines (including anonymous hot lines).”

Hot lines that satisfy the requirements of both the U.S. sentencing guidelines and the OIG program guidance can be operated in house or through an outside firm. For many organizations, it is neither cost effective nor service effective to operate their hot line internally.

The key factor to consider is the anticipated call volume. On average, the hot line call volume will amount to an equivalent of approximately one to two percent of the employee population annually. The volume will vary depending on advertising, employee confidence, and current issues affecting the company. Divide that number by 12 and you get the monthly average. Divide the number by 50 and you arrive at the expected weekly average.

What becomes apparent to most companies is that it may not be cost effective to operate the hot line internally. Furthermore, attempting to utilize existing resources to run a hot line may result in an ineffective, problem-plagued operation. Therefore, outsourcing this function...
may be an appropriate option for many companies.

There are several factors that could lead many small to midsize organizations to outsource the function. Those factors include the following:

■ Only properly trained and skilled operators should debrief callers.
■ Voice mail will compromise anonymity by recording the caller's voice.
■ Live operators are much more likely to elicit important information.
■ Hot line operators should not be distracted by other duties.
■ Employees must be available to receive calls when they are made.

■ Weigh the overhead cost of in-house staff in calculating costs.
■ Calls to an in-house hot line are difficult to “blind” from being traced.
■ Vendor cost is between 5 and 15 percent of the cost of in-house operation.
■ Vendors can provide 24/7 coverage, 365 days of the year.
■ In-house operations are hampered by employee vacation, sick time, et cetera.
■ Competent vendors provide expertise to ensure proper handling of calls.
■ Using vendors permits better use of resources to investigate call reports.
DOJ Issues Revised Principles for Prosecuting Corporate Fraud

The Impact on Settlement Negotiations with the Federal Government

On December 12, 2006, the U.S. Department of Justice (DOJ) issued revised principles for prosecuting corporate fraud to be used by federal prosecutors in conducting investigations, determining whether to bring charges, and negotiating plea agreements with corporate “targets.”¹ The revised principles, which took the form of a 19-page memorandum from Deputy Attorney General Paul McNulty entitled “Principles of Federal Prosecution of Business Organizations” (otherwise known as the “McNulty Memorandum”), were issued in part to address considerable and persistent criticism of earlier guidance issued to federal prosecutors on January 20, 2003, by then-Deputy Attorney General Larry Thompson (also known as the “Thompson Memorandum”).

The contents of the McNulty Memorandum may influence the way that health care organizations design and implement compliance programs, conduct internal investigations, consider self-disclosure options, interact with in-house and outside counsel, and conduct settlement negotiations with the federal government.

The Justice Department’s Principles for Prosecuting Corporate Fraud — An Overview

Like the Thompson Memorandum before it, the McNulty Memorandum provides a set of general principles for Justice Department prosecutors to consider when making decisions about whether to prosecute business organizations. In large part, these factors are the same for corporations as they are for individuals. The McNulty Memorandum warns that corporations should be treated neither more leniently, because of their artificial nature, nor more harshly than individual wrongdoers. There are, however, certain additional factors due to the
unique nature of corporations that federal prosecutors are instructed by the McNulty Memorandum to take into account when reaching a decision as to the appropriate disposition of corporate misconduct.

For example, prosecutors “must consider” the following:

- The nature and seriousness of the offense, including the risk of public harm and any special policy concerns;
- The pervasiveness of wrongdoing within the corporation, including the extent to which management condoned or was complicit in the alleged misconduct;
- The corporation’s past history, such as prior criminal, civil, or regulatory enforcement actions that may evidence a corporate culture of noncompliance;
- The value of the corporation’s cooperation, including voluntary disclosures and the willingness to provide relevant evidence to the government;
- The existence, adequacy, and effectiveness of any pre-existing corporate compliance program;
- The corporation’s remedial actions, including meaningful efforts to implement or enhance a compliance program, pay restitution, and take appropriate disciplinary action with respect to responsible management and other personnel;
- Potential collateral consequences of charging the corporation, including non- penal sanctions such as the federal government’s ability under certain circumstances to exclude a corporation from participation in federal health care programs or to debar it from eligibility to engage in government contracting;
- The adequacy of taking enforcement action against responsible individuals alone rather than the corporation; and
- The existence and adequacy of noncriminal alternatives, such as civil or regulatory enforcement actions.

**CRITICISM OF THE THOMPSON MEMORANDUM**

Although much of this guidance is taken directly from the Thompson Memorandum (in part, verbatim) and even earlier pronouncements by the DOJ to federal prosecutors, the DOJ characterizes the McNulty Memorandum’s criteria with respect to one of these factors, gauging the extent of the corporation’s cooperation, as significantly modified in response to criticism of the Thompson Memorandum from an unlikely coalition of business groups, former senior DOJ officials, corporate and defense counsel, bar associations, civil rights advocates, and Capitol Hill.

In particular, the Thompson Memorandum, which was issued during a recent era of several large corporate accounting scandals viewed as indicative of unfettered corporate greed, permitted federal prosecutors to consider whether the company agreed to share privileged communications with the government in assessing the scope and value of a company’s cooperation.

Another factor to be considered by prosecutors under the Thompson Memorandum was whether a company had paid its employees’ legal defense fees beyond what was required by law. Critics of these Thompson Memorandum policies claimed that they created a “culture of waiver” pursuant to which companies felt forced to waive important legal rights and protections in order to avoid criminal prosecution and obtain the best possible civil settlement.

**CHANGES EFFECTED BY THE MCNUULTY MEMORANDUM**

The McNulty Memorandum, which was announced by Mr. McNulty in a speech before a meeting of the Lawyers for Civil Justice, was meant in part to counter these criticisms. To that end, the McNulty Memorandum instructs that prosecutors should be “mindful of the common cause we share with responsible corporate leaders,” that “confidence in the [Justice] Department is affected both by the results we achieve and by the real and perceived ways in which we achieve them,” and “our willingness to secure the facts in a manner that encourages corporate compliance and self-regulation... impacts public perception of our mission.”
The vast majority of principles remain unchanged from the Thompson Memorandum. The McNulty Memorandum does, however, alter the DOJ's approach to the waiver of attorney-client privilege and work product protection during the course of corporate fraud investigations. The revised principle for assessing "the value of the cooperation" creates a process that prosecutors must follow before requesting that a corporation waive these legal protections.

Although the McNulty Memorandum continues to acknowledge that waiver of privilege may expedite a government investigation, it specifically states that waiver is not a prerequisite to finding that a corporation has cooperated. Under the revised guidelines, prosecutors only may request privileged information after (1) making a determination that there is a legitimate need for such information and (2) following a step-by-step approach for making the request that involves more senior DOJ officials.

Under this step-by-step approach, prosecutors first must seek purely factual information, called "category I" information (e.g., internal documents, witness interviews and factual summaries, and fact chronologies or reports documented by counsel). Before requesting that a corporation waive any attorney-client or work-product privilege associated with category I information, the prosecutor must obtain the written authorization of the U.S. attorney, who may only grant or deny such authorization after consulting with the assistant attorney general for the Criminal Division at the DOJ. It is important to note that a corporation's decision whether to waive privilege with respect to category I information may continue to be used to determine the level of the corporation's cooperation in the government's investigation.

Only if category I information "provides an incomplete basis upon which to conduct a thorough investigation" should prosecutors seek to obtain a waiver of privilege for "category II" information, which is identified as attorney-client communications or nonfactual attorney work product (including documents containing an attorney's mental impressions or legal advice). Prosecutors are cautioned to seek this type of information only in rare circumstances and, before they do so, first must obtain, through the U.S. attorney, the written authorization of the deputy attorney general of the United States.

Unlike with category I information, a corporation's decision not to waive privilege with respect to category II information may not be used to evaluate the corporation's willingness to cooperate with the government investigation; i.e., the decision not to waive the privilege associated with category II information may not be used when the prosecutor is deciding whether to charge a corporation.

In addition to revising the approach taken to the waiver of privilege issue, the McNulty Memorandum also states that a corporation's advancement of legal fees on behalf of employees generally should not be taken into account in making prosecution decisions. It only would be appropriate to do so if the advancement of fees, combined with other "significant facts," demonstrates that the action was intended to impede the government's investigation. Under such rare circumstances, fee advancement may be considered only if authorized by the deputy attorney general.

**Likely Impact of the McNulty Memorandum**

The McNulty Memorandum was issued in direct response to the growing and expressed concern that communications between corporations and their legal counsel were being hindered by a fear that such communications, and the ensuing legal advice received, eventually would be turned over to the government to show full cooperation with an investigation or to avoid criminal prosecution. If the McNulty Memorandum's revised guidance to federal prosecutors is im-
plemented as stated, it is clear that the government intends that corporations should feel less reticent to have candid and complete discussions regarding compliance issues with their legal counsel (and in turn will be provided more complete and accurate legal advice) if there is greater confidence that the attorney-client privilege and attorney work product protection will be respected.

That said, some critics continue to caution that simply requiring approval from the local U.S. attorney or a higher-level supervisor at the DOJ does little to prevent prosecutors from making unjustified requests for waiver of privilege that will continue to chill attorney-client communications. Moreover, even if failure to provide category I information is not penalized, the affirmative decision to waive the attorney-client privilege still may be given favorable consideration under the McNulty Memorandum in determining the corporation's level of cooperation, thereby lessening the impact of the revised guidance and perpetuating the culture of waiver. Finally, the McNulty Memorandum fails to address other contentious issues in dealings between the federal government and target corporations, such as the status of joint defense agreements and the information shared pursuant thereto.

One thing, however, is quite clear — both the Thompson and the McNulty Memoranda consistently place significant emphasis on preexisting compliance programs in making a charging decision. The mere existence of a corporate compliance program, however, is not sufficient, in and of itself, to justify not charging a corporation.

Prosecutors are directed to take the effectiveness of a corporation’s compliance program into consideration and to determine whether it’s merely a “paper program” or whether it was designed and implemented in an effective manner. In making that assessment, prosecutors should consider such things as whether (1) “corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives;” (2) “the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation’s compliance efforts;” and (3) “the corporation’s employees are adequately informed about the compliance program and are convinced of the corporation’s commitment to it.”

**Conclusion**
Given the focus of many U.S. attorneys’ offices around the country on investigating corporate health care fraud, the guidance to federal prosecutors provided by the McNulty Memorandum is particularly relevant to the health care industry. Industry participants should take some comfort in the revised guidance with respect to assessing a corporation’s cooperation in a government investigation but should keep in mind the factors that prosecutors are directed to consider when investigating corporate misconduct, determining an appropriate resolution, and negotiating settlement. In particular, health care companies would be well advised to assess the effectiveness of their corporate compliance programs in light of the McNulty Memorandum and address in advance any weaknesses that exist.

**Endnotes:**

1. The guidelines apply to a federal prosecutor’s consideration of the appropriate disposition with respect not just to corporations but to “all types of business organizations, including partnerships, sole proprietorships, government entities, and unincorporated associations.”
2. For example, when determining whether to charge a corporation with an antitrust violation, the DOJ’s Antitrust Division only will give favorable consideration with respect to responsible pre-indictment conduct to the first corporation to make a full disclosure to the government.
3. For example, U.S. District Court Judge Lewis A. Kaplan struck down as unconstitutional those provisions of the Thompson Memorandum that permitted federal prosecutors to consider

*CONTINUED ON PAGE 68*
Those Who Seek to Establish Compliant Behavior May Very Well Be At Odds With Our Culture

When I was a teenager, I ran with a pretty assertive pack. When we infringed on someone else's personal space, we would often say, “Excuse you for bumping into me.” In other words, we blamed it on the other guy.

My family and I were just on vacation, and I had a flashback to those times. I was in a crowded restaurant, and a lady who was not watching where she was going plowed right into me. She exclaimed, “Excuse you!” I just stood there speechless, which is a rare thing for me.

The next day, I was helping my 5-year old daughter, who is the model of grace and manners (really) to get some fruit at the breakfast buffet. Two young hooligans plowed in with their mom in tow and elbowed us out of the way. They did manage to tell us, “Sorry you are in the way.” Are these isolated instances or simply the way things are going in our society? Do we have an accountability crisis?

During the same vacation, I was reading news stories about the firings of a number of U.S. attorneys across the country. Congress was, and still is, giving the White House, the attorney general, and others a lot of heat over those firings. The attorney general publicly stated that he did not intend to resign but said, “I acknowledge that mistakes were made here.”

Later, the President said that he supported the attorney general but that he was “frankly not happy about” the way the attorney general handled the matter. He denied that the firings were politically motivated, instead complaining, “What was mishandled was the explanation of the cases to Congress...”

What did the President mean? Was he lamenting that nobody paid attention to developing a palatable expla-
nation for the firings or at least plausible
deniability? We can never know. Indeed, there was no indication of what the mis-
takes might have been, or by whom they might have been committed. It is impos-
sible to glean any meaning when analyzing this fragment of a phrase, especially be-
cause it is uttered in the passive voice.

Before you accuse me of singling out re-
cent political events or certain politicians, I need to point out that countless politicians have engaged in this kind of wordsmithing. It is not limited to the example at hand. In fact, this approach goes way back.

The phrase is most often attributed to President Nixon. Others adopted it later. Re-
member President Reagan and the contras? At the time, the Vice President (the dad of the current President) said “mistakes were made.” Years later, when accused of violating federal travel rules, a senior political appointee kept the mantra going by admit-
ting that “mistakes were made.

This is not limited to political matters, however. Even the people behind infor-
cercials have adopted voluntary codes of conduct and named compliance officers after admitting that “mistakes were made” in the claims they made on the late-night airwaves.

The diffusion and misallocation of re-
sponsibility found in “I am sorry if you were offended” also goes way back. Re-
member the “costume failure” during the Super Bowl a few years ago? One of the performers expressed regret to the extent people were “offended” by the incident.

The same thing happens with software companies. When there is a glitch that is hard to fix, they often label it a “known is-
sue” instead of admitting the shortcoming. One of my favorites is a statement by for-
mer New York Mayor Ed Koch, speaking in 1987 about remarks he made about a bor-
ough president: “If I’ve insulted him in the past, then I’m sorry, and I withdraw my re-
marks. But I can’t think of any.”

Whether the phrase is “excuse you for bumping into me,” or “mistakes were made,” or “I am sorry if you were offended,” the meaning is the same. None of these statements expresses any kind of remorse or contrition. The speaker states only that he is sorry that the situation happened — mostly because it somehow inconve-
nienced him. There is no accountability inherent in the declaration. There is no offer to make things right.

The dilemma here is that those who seek to establish compliant behavior are at odds with our culture. Our leaders cannot admit even a single mistake. We are made to feel guilty when others bump into us or elbow us out of the way. If we are offended by someone else’s behavior, then our stan-
dards must be out of whack. Nobody is ac-
countable for anything.

If something does not go our way, we try to hold somebody else responsible, and we often feel they should have to pay. Liter-
ally. Yet we ourselves often refuse to admit fault or make amends. Against this back-
drop, can we truly hope to have effective compliance programs in accordance with the established elements? Or are we just beating our heads against the wall in a cul-
ture that simply does not care? More about that next time.
Update on NPI Implementation: CMS Contingency Plans

Even Entities on Target with the Implementation Date Will Benefit from the Additional Time

With the May 23, 2007, deadline for compliance with the national provider identifier (NPI) regulations approaching, CMS decided to give covered entities some breathing room. Once it became apparent that many entities would not be in full compliance by the deadline, CMS issued guidance on April 2, 2007, announcing an additional 12 months for providers to implement “contingency plans.”

During this one-year extension period, CMS will consider complaints of noncompliance on a case-by-case basis. According to CMS, the agency will not impose penalties on covered entities that deploy contingency plans if they have made reasonable and diligent efforts to be compliant. In assessing an entity, CMS will consider “good faith” efforts at compliance, reasons for noncompliance, planned corrective actions, and related factors during the one-year moratorium on penalties.

The NPI requirement comes from the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Act included a requirement for covered entities to apply for, be assigned, and begin to use a single national provider identifier, and no other provider identifier number, on all HIPAA-covered transactions. Requiring NPIs was one of HIPAA's attempts at industry-wide simplification of health care provision and administration, as well as reduction of fraud and abuse. NPIs are intended to eliminate the need for payors and providers to keep numerous identifiers, which would then simplify transaction processing between these entities.

Prior to the April 2 announcement by CMS of the one-year extension of the enrollment deadline, providers and payors may have noticed a flurry of communications from CMS and commentators warning against “further
procrastination” as something that would “disrupt cash flow.” CMS received numerous inquiries expressing concern over the health care industry’s state of readiness. CMS’ initial responses appear to have caused considerable confusion among providers and payors.

**VIEW FROM THE TRENCHES**

CMS has several online newsletters to which members of the public may subscribe. Free online registration with these “listservs” entitles the registrant to receive periodic email messages related to specified topics of interest. During the weeks just prior to the April 2 extension announcement, the communiqués from CMS to health care providers seemed by some to read as follows:

Dear Provider,

Re: National Provider Identifier: Compliance Date May 23, 2007

Get it; share it; use it. But protect it. And get anyone you deal with to get one.

You should get your NPI if you haven’t. The requirement appeared in the January 23, 2004 Federal Register. The drop-dead deadline was May 23, 2007.

Except that on April 3, 2007, we announced a contingency plan for those of you that won’t make the deadline. If you have been making a good faith effort to meet the deadline, you have another year to “implement contingency plans that could include accepting legacy provider numbers on HIPAA transactions in order to maintain operations and cash flows.”

Although getting an NPI is free, “not having one can be costly.” You can read about it at this live link: http://cms.hhs.gov/NationalProvIdentStand/.

**PRELIMINARY CONSIDERATIONS**

Until more consistent guidance is provided by CMS (“More on NPI Coming Soon…”), the following steps should be considered by covered entities to help show good faith efforts to comply with the NPI provisions of HIPAA.

- All covered entities should apply for an NPI.
- Providers should submit small batches of compliant, NPI-only claims to one trading partner at a time and track whether specific recipients are ready for their compliant claims.
- If compliant claims are denied, providers should consider resubmitting claims using previously acceptable formats or resubmitting claims with both legacy and NPI numbers.
- If noncompliant claims do not receive a rapid response (either denial or payment), providers should consider resubmitting their claims with only NPI numbers as provider identifiers.
- Payors should continue (or begin and continue) outreach and testing efforts and keep records of their continuous attempts at achieving compliance. CMS will “place a strong emphasis on sustained actions and demonstrable progress.” Payors can continue to process payments to providers during this process.

It is unclear whether clean-claims laws require payors to continue paying providers during the contingency plan phase. It is unlikely that CMS intended to overturn prompt payment regulations, but given the sometimes contradictory communications on this issue, providers also should consider strategic, organized claim resubmission procedures to help reduce cash flow disruption.

CMS still needs to provide some critical policies, such as guidance on whether special permission is needed on the exchange of NPIs among covered entities, and other

**CONTINUED ON PAGE 68**
Physician Services “Place of Service” Reporting: Why All Providers Should Be Concerned

Review Computerized Billing Systems and Ensure Staff Understand Implications of Improper Reporting

Outpatient services may be provided in a number of different settings: the physician office or clinic, an outpatient service area of a hospital, in an ambulatory surgery center, or in another free-standing facility. When a physician provides outpatient services, a majority of payors (including Medicare Part B) base a portion of the reimbursement for certain services on a data element known as the “place of service.” This indicator is found on the CMS-1500 claim form for professional (physician) services, and the appropriate choices include the following:

- 11 (physician office);
- 22 (outpatient hospital); or
- 24 (ambulatory surgical center (ASC)).

For a physician to receive the higher nonfacility practice expense payment for a service, the service must meet the requirements of 42 C.F.R. §414.22(b)(5)(i)(B):

The higher non-facility practice expense RVUs [relative value units] apply to services performed in a physician's office, a patient's home, an ASC if the physician is performing a procedure not on the ASC approved procedures list, a nursing facility, or a facility or institution other than a hospital or skilled nursing facility, community mental health center, or ASC performing an ASC approved procedure.

CMS publishes a physician fee schedule in the Federal Register showing those services having a higher payment rate if performed in a physician's office.

If a physician provides the service in his or her office setting, it is assumed that additional overhead costs will be in-
curred, and the reimbursement is increased if the place of service indicator is designated as “physician office.” If the place of service is incorrect on the physician claim form and the other provider (such as a hospital outpatient department or an ambulatory surgery center) also submits a claim, overpayment or payment duplication may result.

This issue should be of concern to physicians, practice managers, and compliance staff of all providers. There is a definite compliance risk for the professional services (physician) providers, and there is the possibility of current or future underpayment for those service sites where the services were provided and that assumed the overhead costs of providing them.

In December 2006, the Office of Inspector General (OIG) released a report entitled “Review of Place of Service Coding for Physician Services Processed by National Heritage Insurance Company During Calendar Years 2002 and 2003.” The report detailed the findings from a study performed on a 100-claim stratified random selection of physician service claims, 70 of which may have been performed in an outpatient hospital setting and 30 of which may have been provided in an ambulatory surgical center.

National Heritage Insurance Company is the Medicare Part B carrier that processes and pays claims submitted by Part B providers in Massachusetts, Maine, New Hampshire, Vermont, and California. The results are summarized in Figure 1.

Physician service providers inappropriately coded the place of service designation on 81 of the 100 claims reviewed. As a result, the Medicare carrier overpaid the physicians $5,423; when this figure was extrapolated over the population of claims for the time period reviewed, it was estimated that an overpayment of approximately $4,254,613 resulted.

The methodology utilized during the study included the following:

- Reviewed applicable Medicare laws and regulations;
- Identified services coded as being performed in a physician's office that were at high risk for overpayment because the coding would result in a higher payment to the physician;
- Matched claims from physicians for high-risk services to claims from hospital outpatient departments or ASCs for the same services performed on the same beneficiary on the same date;
- Selected a stratified random sample of 100 paid services that represented services that had a high risk of payment error;
- Reviewed the common working file and paid claims for the sampled services to validate the amounts of payments to physicians and other providers and to determine the place of service for which the services were paid;
- Sent a detailed internal control questionnaire and request for medical and billing records to 85 physicians who provided the sampled services;
- Reviewed medical and billing records and, in some cases, followed up with physicians or their billing agents to request additional information to confirm the place of service, identify coding discrepancies, and identify the underlying causes that contributed to incorrect designation of place of service;
- Followed up with hospital outpatient and ASC providers to verify that the

---

**Figure 1: Summary of Results**

<table>
<thead>
<tr>
<th>Stratum</th>
<th>Description</th>
<th>Sample Size</th>
<th>Number of Errors</th>
<th>Value of Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Physician — outpatient hospital setting</td>
<td>70</td>
<td>51</td>
<td>$1,726.69</td>
</tr>
<tr>
<td>2</td>
<td>Physician — ambulatory surgical center</td>
<td>30</td>
<td>30</td>
<td>$3,696.29</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td><strong>$5,422.98</strong></td>
</tr>
</tbody>
</table>

CONTINUED ON PAGE 69
Compliance Professionals Often Have to Focus Their Resources on Areas That Pose the Greatest Risk

Carefully Budget Time Spent on Issues That Are Either Low Priority or Perhaps No Longer Relevant

Risks for entities, including laboratories, are constantly evolving. What was considered a risk area yesterday may not be today for a variety of reasons. In some cases, a risk area changes because the rules have changed or because government focus has changed. In others, it is because the entity, the industry, or technology has changed and adapted, and the risk area is no longer a risk area. Compliance professionals must make sure their often limited resources and time are used to address issues that present risks today, rather than doing things that were a risk area previously but may not be now.

I have had a series of recent inquiries concerning two items that were published in the 1998 Office of Inspector General (OIG) Compliance Program Guidance for Clinical Laboratories. These two items were considered important at the time the guidance was published but are not so important today, and yet they continue to consume the time and energy of laboratory compliance officers — time and energy that could be better applied to issues that are important today. These two items are annual notices to clients and monitoring the utilization of test orders.

BACKGROUND

At the time the original laboratory compliance guidance was published, the industry was in the throes of prosecutions and subsequent settlements related to bundling and unbundling of tests, including separately billable tests in panels that were not separately identified or ordered and the use of custom panels. The government contended that labs were causing unnecessary tests to be ordered through a variety of mechanisms and tactics without the physician being fully aware of the bill-
ing consequences of these orders. Many of the risk areas identified in the compliance guidance were based on that activity and the government’s focus on that activity at that time.

There were several risk areas identified in the guidance and several comments on what labs should be doing to prevent these unnecessary test orders. Requisition design, full disclosure and acknowledgements for custom panels, documentation of the medical necessity for all tests ordered, and other measures were discussed in the guidance. Most of these are still applicable today. The guidance also suggested that laboratories publish annual notices to physicians that basically outline Medicare rules for the ordering and billing of tests and that labs monitor the utilization of their services to detect any inappropriate utilization patterns that they inadvertently may have caused.

**ANNUAL NOTICES**

First, there is no law or regulation requiring labs to send such notices, yet many labs feel that this is a “requirement” the OIG has set for them. The government publishes its rules and regulations in many places, and it is the responsibility of all providers to be aware of the ones that affect them.

Secondly, and most importantly, there is no evidence to suggest that these annual notices have any impact on the ordering behavior of physicians. There are many tangible benefits to keeping your physician clients current on billing and other compliance-related issues, but sending a long and often redundant annual notice is probably not going to accomplish those benefits.

Most labs send information and notices throughout the year as things change. The savviest labs coordinate their notices with the quarterly changes that CMS makes to the laboratory national coverage decision database, correct coding initiative changes, and other rules and reimbursement issues. Many important system changes occur at the quarters. These notices take the form of newsletters or other eye-catching tools that help increase the chances they will get reviewed.

Also, most labs include a section in their user guide or Web site that provides the OIG-suggested contents for the annual notice and update it each time the guide or Web site is updated. These existing activities meet the suggestion in the guidance for annual notices.

All labs need to do is keep a file or record of everything sent throughout the year and, if the labs want to, send a one-page letter each year that reminds its clients where the compliance information can be found and to watch for the quarterly notices and updates. This is a more effective way to communicate, is integrated into currently existing processes, and consumes little or no additional resources.

**MONITORING TEST UTILIZATION**

In the compliance guidance, the OIG suggests that labs should be careful not to do things that cause the ordering of unnecessary tests and recommends the lab monitor the utilization of its services. The guidance gives an example of an annual monitoring technique that, if viewed objectively and with a knowledgeable eye, has little or no chance of accomplishing the desired outcome. If a laboratory is engaged in some form of this example on an annual basis, it is a waste of time and effort because it affords no real protection.

Here is what the lab should do with this. When the laboratory makes a change that could affect ordering of tests, such as adding a new test or changing a methodology for an existing test, it should analyze the potential for the change to affect test orders. If there is a possibility of orders being affected, it should monitor the ordering of the tests involved at an appropriate interval after the change to make sure that there was no change in methodology or that any change that occurred was an appropriate change. This could be one or two months...
for a high-volume test or six months for a lower-volume test. Let's look at a case to illustrate this concept.

A laboratory decides to add a new, high-sensitivity thyroid-stimulating hormone assay because it is a more sensitive and specific test than the tests the lab currently uses to diagnose and follow treatment of thyroid disease. The new test is supposed to supplant two existing tests that are commonly used for the condition.

When the new test becomes available to its clients, the lab sends a letter to its clients touting the benefits of the new test and instructs them to use the new test in place of the two older tests that are now used. The laboratory checks after a month of the new test's availability and finds that it is being ordered at a volume that is about what it expected based on the usage of the old tests, but it also finds that the volumes of the older tests have not dropped off to the extent expected and, in many cases, they are being ordered on the same patient.

With those findings in hand, the lab needs to take some action to correct the problem. It should analyze the unnecessary referrals and take appropriate action based on the findings of the analysis.

This is what the guidance document is talking about, and taking this approach assures that any resources spent on test utilization monitoring have value.

Summary
This column uses the two examples of annual notice and monitoring utilization of lab services as examples of activities that, if they are an area of focus for a laboratory compliance officer, should have a lower priority. Laboratory compliance officers would be better off focusing on areas like Stark and anti-kickback regulations and Medicaid billing if they have to choose where to focus resources.

Compliance is a dynamic and evolving, almost living thing that requires care and maintenance by thinking compliance professionals who are attuned to current issues and problems for their areas of responsibility. Resource and fiscal constraints force compliance professionals to focus their resources in the areas that are going to have the most impact on the most important issues of the day, the ones that pose the greatest risk, rather than spending those precious resources doing things that have no real value in today's compliance world.

Endnotes:

Gustin

implements an electronic medical record (EMR) system that either allows or prohibits access inaccurately within the system. This could lead to users having the ability to order diagnostic or therapeutic tests without being licensed to do so. In addition, depending on how the user's roles and responsibilities are defined, there is the potential that bills could be mistakenly submitted for services that are outside the scope of one's practice.

It is critical that allied health professionals provide only those services that are within their scope of practice. Furthermore, their services should only be reported when the appropriate regulations and provisions have been met. The type of allied health professional, the state in which the services are rendered, and the specific payer regulations need to be carefully reviewed in order to determine what services they can provide, where the services can be provided, and under what circumstances such services can be billed to a payer.

Endnotes:
sure, skills, and training when credentialing caregivers.

Snell: If you moved out of CMS into a role as a compliance officer for a provider, what would be the first thing you would do?

Brandt: My first task would be to conduct an overall assessment of the organization's compliance effectiveness program. Within this evaluation, it would be critical to determine the compliance officer's interactions with people throughout the organization. How well an organization's compliance officer is integrated into the organization has a tremendous impact on the overall effectiveness of the program.

Snell: Do you have any advice for compliance officers who undertake an effectiveness assessment of their organization?

Brandt: Compliance officers should be vigilant about ensuring that compliance is part of the culture of the organization.

Snell: Are there any guidances or templates that would assist an organization in conducting an effectiveness assessment?

Brandt: As previously stated, at the completion of the compliance effectiveness project, CMS will release a lessons learned document later this spring that will provide sound techniques for developing and maintaining an effective compliance program. Our recovery audit contractors (www.cms.hhs.gov/RAC) and comprehensive error rate testing (www.cms.hhs.gov/CERT) reports, however, are currently available, and these are tools that can help an organization mitigate potential risks.

Snell: How often would you recommend an organization conduct an effectiveness assessment of its compliance program?

Brandt: At a minimum, a program audit should be conducted at least yearly. Organizations should consistently assess their programs for areas of improvement. Ideally, organizations would reevaluate their program when new information is released by government agencies or other counterparts in the industry.

Snell: How would you define an effective compliance program?

Brandt: An effective compliance program is one that focuses on detecting and identifying potential problems before they occur. Once a potential vulnerability is identified, an effective program will have appropriate processes and strategies in place to mitigate or correct the problem and prevent the same problem from occurring again.

Snell: What role should the organization's board play in overseeing the compliance program?

Brandt: This would vary depending on the type and size of the organization, but the board should oversee and provide direction for the organization's compliance program. The most important role of the board is to ensure that compliance is fully integrated within the culture of the organization.
**Snell:** When do you expect a company to disclose information about a potential violation to you?

**Brandt:** This information should be disclosed to CMS as soon as the potential violation is identified to ensure that Medicare Trust Fund monies are not paid inappropriately and that any inappropriate payments are recommended for recoupment.

**HIPAA**

variety of forms. In some cases, the PHR contains patient health information extracted from the EMR used by a covered entity. In those cases, any information that flows from the EMR of a covered entity to a PHR of a noncovered entity is PHI, disclosure of which should be subject to the HIPAA privacy and security rules.

HHS has not yet provided any guidance on how disclosures of information from the EMR of a covered entity to the PHR of a noncovered entity should be handled with respect to HIPAA, but it appears these types of disclosures could be covered by one of the following HIPAA privacy rule standards:

- 42 C.F.R. §164.506 Uses or disclosures to carry out treatment, payment, or health care operations;
- 42 C.F.R. §164.508 Uses and disclosures for which an authorization is required;
- 42 C.F.R. §164.524 Access of individuals to protected health information.

If the transfer of PHI from the covered entity’s EMR to the noncovered entity’s PHR is considered a disclosure for which an authorization is required (§164.508), then the covered entity must obtain written authorization for the disclosure of PHI to the PHR vendor. All the provisions covering the requirements of a valid authorization apply, such as specification in the authorization of what information may be disclosed, to whom it may be disclosed, a termination date or event, the right to withdraw authorization, et cetera.

If the transfer of PHI from the covered entity’s EMR to the noncovered entity’s PHR is considered a disclosure that falls under provisions contained in §164.524 governing individuals’ access to PHI, then the transfer (disclosure) may only be made at the request of the individual and may be made to meet the requirement of that section that “…[t]he covered entity must provide the individual with access to the protected health information in the form or format requested by the individual, if it is readily producible in such form or format.”

Any transfers of PHI from a covered entity to a PHR vendor not covered by the HIPAA rules that were not done in compliance with one of the above provisions of the HIPAA privacy rule would constitute a HIPAA violation.

In the past, HHS has acted in accordance with the recommendations of NCVHS. It is likely that in the next few years, as the national health information network becomes a reality and more and more of our PHI is collected in and accessed through online PHRs, HHS will expand HIPAA privacy rules to cover PHI wherever it resides. Far-sighted covered entities would be wise to keep this in mind as they begin to move their patients’ sensitive personal health information beyond the confines of internal EMRs and into online PHRs, regardless of who owns the technology.
from being able to cover the cost of care.\(^{11}\)

Physicians are concerned that the proposed budget does nothing to address issues related to reduced fee schedules. Providers were encouraged after the passage of December’s Tax Relief and Health Care Act of 2006, which eliminated the 5 percent reduction in physician payments that was anticipated for 2007 and implemented new pay-for-performance incentives. In fact, they hoped that the new budget would go even further by eliminating additional planned reductions in their fee schedules, but it did not. A 10 percent reduction to the physician fee schedule will take place in 2008, as planned.\(^{12}\)

Some Democrats have expressed opposition to the proposed budget. Rep. Pete Stark (D-Cal.), chair of the House Committee on Ways and Means’ Subcommittee on Health, expressed a concern that efforts to increase competition by reducing federal spending cater more specifically to the needs of for-profit corporations. Other committee Democrats disapprove of the Administration’s proposal allowing a tax deduction for couples or individuals who purchase their own health insurance. They argue that this deduction would put those who enroll in employer-sponsored health plans at a disadvantage while benefiting only higher-income individuals and families who can afford to purchase insurance.\(^{13}\)

The ultimate reality is that health care costs are on the rise, and the federal government’s current rate of growth of health care expenditures may outstrip its ability to cover those costs reasonably and responsibly. Not everyone will be satisfied by changes made to the health care system, though changes are clearly needed. What remains to be seen is whether Congress will approve the Administration’s proposals and whether the proposed changes will have the desired effect of providing better health care.

Endnotes:
2. Id. at 2.
3. Id. at 3.
4. Id. at 59, 51.
5. Id. at 2-5.
6. Id. at 54.
7. Id. at 60-61.
9. Id. at 2.
10. HHS Budget in Brief at 53, 55, 58.

Compliance Officer
CONTINUED FROM 44

Now, as of December 2006, IHI has launched the “5 Million Lives Campaign” to prevent needless harm. Among the tenets of the latter campaign is “Getting Boards On Board,” which focuses expressly on the obligation of the directors of health care institutions to take direct responsibility for the quality of care rendered by their organizations. It is no longer enough for health care organizations to mouth the truism that “quality is job one.” The measures of demonstrated performance are real; they are clear; and they have teeth.

What is a compliance officer to do? In the spirit of independent compliance reporting, raising the consciousness of the board and administration of a health care entity to these quality mandates is now a critical task, at least as compelling as improving their technical billing compliance sensitivity. The liability of boards on these issues is far greater than even five years ago.\(^{8}\)

Helping them understand that there are many significant opportunities within the
boundaries of the Stark and anti-kickback statutes for hospitals and physicians to work together in common cause for quality in ways that benefit the physicians financially will advance the hospital’s cause.9 There are many quality-focused strategic initiatives with compliance implications. For all health care industry sectors concerned about compliance, compliance officers should review the OIG’s last four years’ work plans to understand the quality-relevant initiatives currently underway.

How can a compliance officer effectively integrate quality-oriented issues into workflow? Develop a strategy to work with the risk management and quality improvement departments to determine where compliance ought to be involved. Think about how standardization of care in accordance with good clinical practice guidelines can bolster and support the likelihood of meeting the new standards.10 Participate in efforts to monitor such concordance.

Quality data ought to be a critical focus of attention. Become familiar with the quality metrics, report card, and transparency initiatives applicable to your enterprise. Find out who is reporting what and to whom. Develop effective techniques to monitor these reports over time for accuracy, completeness, and as bellwethers for other problems in the organization. Quality data liabilities are the big iceberg here; not only are they now the bases for compliance liabilities on their own, but identified quality failures often point to other process problems.

In the last analysis, the new world order in health care is patient centric and quality driven. Compliance is no longer just about money. Its inescapable connection to quality is vital to the essential purpose of the health care enterprise — whatever type of business that might entail.

Endnotes:
5. 42 U.S.C. §1320 a-7a(a)(3).
6. 42 U.S.C. §1320 a-7-a(b).
security safeguards. Training standards are specific in the HIPAA rules and normally are accomplished by combining privacy and security training in a way that covers all aspects of compliance.

Proper training of orientees in any position (e.g., employees, physicians, volunteers, vendors) prior to PHI access is supportive of privacy maintenance. Any process that reminds and helps keep privacy and security practices top-of-mind assists busy people who want to do what is right to comply more consistently. Now, and as policies and procedures change to adapt to a changing industry landscape, technology functions offer significant help with guiding compliance, featuring ongoing reminders, alerts, et cetera.

It is well known that training needs to be customized to a role to equip an individual with the knowledge needed to uphold an organization’s privacy requirements for specific responsibilities. An example is the influence position frontline staff members are in when fully trained to educate the public one-on-one. Understanding the bigger picture may help make the case for “we're all in this together.” Do they understand the industry enforcement process, organizational risks, and reputation issues with public exposure should privacy and security efforts falter?

**CONCLUSION**

By keeping watch on developing initiatives through transitioning times, privacy and security officials can be a strong influencing voice on privacy and security trust factors in health care. They know the issues. They experience the industry gaps and interpretation fog on a day-to-day basis. They are in a position to keep asking insightful questions and to apply lessons learned through their involvement. They can influence development of legislative drafts and policy setting for the evolving future of health care.

For additional information, or to obtain a copy of the “On the Front Lines of Healthcare Privacy” report, go to www.ahima.org.

**Settlements**

Continued from 54

whether the corporation advanced legal fees to its employees. *U.S. v. Stein*, 435 F. Supp. 2d 330 (S.D.N.Y. 2006). Moreover, as outgoing chairman of the Senate Judiciary Committee, Sen. Arlen Specter (R-Pa.) introduced legislation in December 2006 to overturn the Thompson Memorandum policy allowing prosecutors to consider whether the corporation waived the attorney-client privilege in assessing cooperation.

**National Provider Identifier**

Continued from 58

data dissemination policies. Covered entities are expected to benefit from any expansion of education and outreach efforts by CMS. Lessons learned from NPI implementation can perhaps guide adoption of other transactions standards to manage implementation costs.

The new guidelines should be seen as good news for covered entities. Even entities on target with the implementation date can benefit from the flexible enforcement approach and additional time provided in making a smoother transition.

**Endnotes:**

1. The deadline is May 23, 2007 — except for small health plans, which must be in compliance by May 23, 2008.
3. Id. CMS encourages “voluntary compliance” and will use a “complaint-driven approach for enforcement.”
6. Id.
7. NPI Frequently Asked Questions, www.cms.hhs.gov/NationalProvIdentStand/07_Questions.asp#TopOfPage (last visited April 6, 2007) (“I have been told to protect my [NPI], and I have been told
sampled services were performed at their facilities;

- Calculated the amounts of any Medicare overpayments for the sampled services;
- Reviewed the common working file to ensure that claims with payment errors subsequently had not been adjusted; and
- Used a statistical projection to estimate the total value of erroneous claims.

An example of the effect of an incorrect place of service designation follows:

A physician was paid $406 for a colonoscopy coded as being performed in his office. The analysis showed that the physician actually performed the service in the ASC and should have received a payment of $200. As a result, the physician was overpaid $206.

It was determined that physicians and their billing agents coded place of service incorrectly for one or more of the following reasons:

- Billing personnel or billing agents were confused about the precise definition of a "physician's office" or were simply following established practice in applying the office place of service code.
- Billing agents were unaware that incorrect place of service codes could affect Medicare payment for a specific code.
- Staff made isolated data entry errors.
- Undetected flaws in the design or implementation of some billing systems caused all claims to be submitted with "physician office" as the place of service.

The physicians and their staff used the office place of service code even though they knew, or should have known, that the service was not performed in the physician's office. Medicare claim form instructions specifically state that each provider or practitioner submitting claims to Medicare is responsible for becoming familiar with Medicare coverage and billing requirements.

As a result of this study, the OIG made the following recommendations:

- The identified overpayments of $5,423 in the sample reviewed should be recovered.
- Work with the physicians who provided the 122,054 services estimated as potentially overpaid by $4,249,190 to determine whether the place of service code was improperly submitted.
- Strengthen the education process and re-emphasize to physicians and their billing agents the importance of correctly reporting the place of service and the need for internal control systems to prevent Medicare billings with incorrect place of service codes.
- Work with the program safeguard contractor to develop a data match that will identify physician services having a high risk for place of service miscoding and to recover resulting Medicare program overpayments.

In the current environment of ever larger health care networks that include both physician and hospital or ASC-based facility providers, appropriate place of service designation is an issue that touches nearly everyone in the medical com-
munity. Those in the compliance arena as well as those personnel responsible for the billing and reporting of each billing component submitted to the Medicare Part B carrier should be aware of the current and ongoing practices of each physician in the network.

Computerized billing systems should be reviewed to ensure that no default value of “11 — Physician office” exists in the place of service field locator without full understanding by billing staff and an ability to override the default value. Significant compliance risk exists related to place of service designation, and each provider of Medicare outpatient Part B services should be aware of the implications of inappropriate reporting.

Endnotes:

We encourage you to use this page to make notes about the articles that appear in this issue of the *Journal of Health Care Compliance*. 
We encourage you to use this page to make notes about the articles that appear in this issue of the *Journal of Health Care Compliance*. 