Journal of Health Care Compliance

Volume 11, Number 4
July–August 2009

Journal of
Health Care
Compliance

Editor-in-chief
Roy Snell

Portfolio Managing Editor
Pamela Carron, J.D.

Managing Editor
Reba Kieke

Coordinating Editors
Susan Smith, J.D., M.A.

Cover Design
Patrick Gallagher

Interior Design
Jason Wommack

Production
Don Torres

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.

Editorial Board

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: $279 per year plus postage, handling and appropriate state sales tax. Single issue price: $56.

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

Permission requests: For permission on how to obtain permission to reprint content, please send an e-mail to permissions@cch.com or FAX 847 267-2516.

Purchasing reprints: For customized article reprints, please contact *FosteReprints* at 866-879-9144 or go to *FosteReprints* website at *www.fostereprints.com*.

Roy Snell

"I Don't Want to Build a World Class Compliance Program"

Extreme Approaches Do Not Help a Company in the Long Run

I was puzzled when Dan Roach recently said this to me, "I don't want to build a world class compliance program." After years of constant effort to improve, I thought Dan was almost on par with my intellectual capacity. This was a big setback to that assumption. After he explained his perspective, my fears of his intellectual demise were momentarily unfounded.

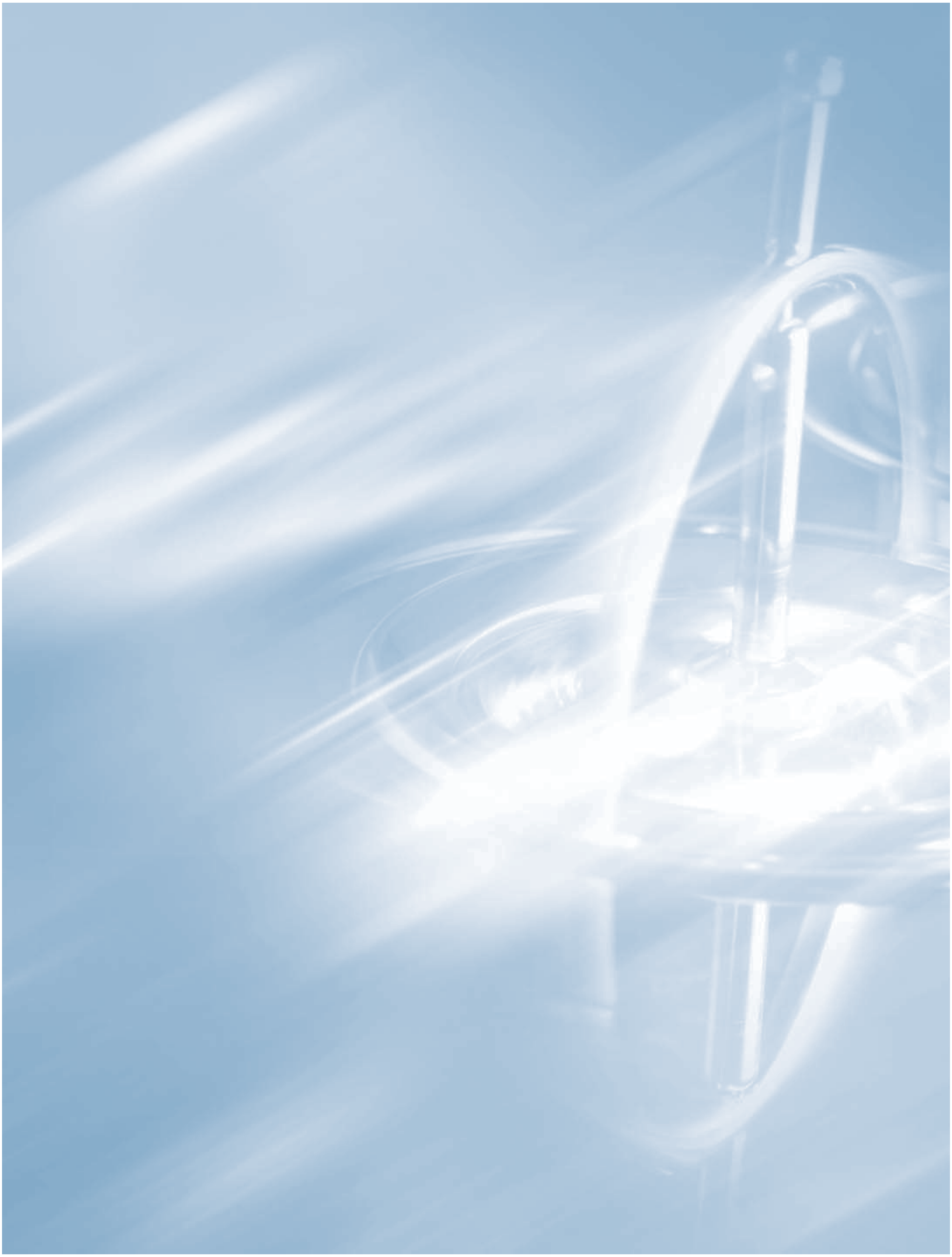
Dan's point was that we should be building a world class organization. We should not be building a world class compliance program or human resources department or audit department or finance department, et cetera. We should be building a world class bank, hospital, manufacturing firm, et cetera and an *effective compliance program*. If every department were to spend the resources necessary to become "world class," the company not only would diminish its chances of achieving its mission and vision but probably would go out of business as well.

Before I go on I need to say that one of the best compliance books ever written is called *Building a World Class Compliance Program,* by Martin Biegelman. When I mentioned Dan's point, Marty said, "I wanted to call the book "*Building an Effective Compliance Program*, but the publisher changed it." Marty agrees with Dan, and despite the publisher's flair for the dramatic, this is a great book.

There are two extremes in any profession: coming up short and overkill. Some people have no clue how to implement a compliance program. They spend their time on ineffective projects and leave their organization exposed. Some request endless resources and run around like Chicken Little over using company resources. Neither approach helps the company in the long run.

Compliance and ethics programs are the most effective tools for dealing with society's request for organizations to follow the rule of law and behave ethically. Our profession will do well. We can prosper on our own merits. We do not need to exaggerate. We do not need overkill. Society's response to Sarbanes-Oxley was overkill. It did not serve us well. Let's all get behind the overarching mission of our organizations and run effective compliance and ethics programs.

Roy Snell is the Chief Executive Officer/Executive Director of the Health Care Compliance Association. Roy is also Co-Founder of the Health Care Compliance Association. Prior to being named HCCA's CEO, Roy was a Director with PriceWaterhouseCoopers in Minneapolis, Minnesota. He began working in the compliance arena when he was named Corporate Compliance Officer for the University of Wisconsin Hospital and Clinics and the University of Wisconsin Medical Foundation in Madison.



HHS and FTC Release Guidance on HITECH Act Requirements for Safeguarding PHI and Breach Rules for HIPAA Covered Entities, Business Associates, and PHR Vendors

Covered Entities Must Update Policies and Practices to Avoid Growing Liabilities

Michael A. Dowell

Michael A. Dowell, Esq., a partner and co-chair of the Health Care Industry Group in the Los Angeles office of the law firm of Theodora Oringher Miller & Richman, is one of the nation's leading health care privacy and security attorneys. Mr. Dowell counsels hospitals and health systems, health plans, insurers, governmental entities, physician organizations, and personal health record vendors with respect to a wide range of privacy and security compliance issues. He can be reached at mdowell@tocounsel.com.

On April 17, 2009, the Department of Health and Human Services (HHS) released guidance to health care providers, health plans, and health care clearinghouses and their business associates (covered entities) about the technologies and methodologies for rendering protected health information (PHI) secure.[1] The HHS guidance will be utilized for purposes of determining when the new data breach notification rules added to federal law under the Health Information Technology for Economic and Clinical Health Act (HITECH Act) will require the covered entity to provide notification of breach of the security of "unsecured protected health information."

On April 16, 2009, the Federal Trade Commission (FTC) released proposed regulations to implement new health information data breach and other health information privacy and security mandates included in the HITECH Act for Health Insurance Portability and Accountability Act (HIPAA) business associates and personal health record (PHR) vendors providing or accessing PHRs and certain other consumer health information.[2] Covered entities and HIPAA business associates covered by the rules will be required to provide certain specified notifications when and if a breach of PHI occurs unless they comply with the applicable HHS or FTC guidance (whichever is applicable) for safeguarding the data.

HHS Guidance to Covered Entities

The HITECH Act required HHS to issue interim final regulations requiring covered entities to provide for notification in the case of breaches of unsecured PHI in accordance with the HITECH Act. Section 13402(h) of the HITECH Act defines "unsecured protected health information" as PHI that is not secured through the use of a technology or methodology required in HHS guidance to render PHI unusable, unreadable, or indecipherable to unauthorized individuals.[3]

When Does a Breach Occur?

A breach of unsecured PHI occurs where there is an "unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of that information, except where the unauthorized person to whom the information was disclosed would not reasonably have been able to retain such information."[4] The HITECH Act includes exceptions to the "breach" definition where: (1) the unauthorized acquisition, access, or use of PHI is unintentional and made by an employee or individual acting under the authority of the covered entity or the business associate if the disclosure or use was made in good faith and within the scope of employment of the person who made the inadvertent disclosure; and (2) an inadvertent disclosure occurs by an individual who is authorized to access PHI at a facility operated by a covered entity to another similarly situated individual at the same facility.

What Must Be Done to Address a Breach?

Under the HITECH Act, a covered entity that has discovered a breach of unsecured PHI must notify each individual whose PHI had been or was reasonably believed to have been accessed or acquired or disclosed in the breach within 60 days after discovery of the breach. If covered entities follow the HHS guidance standards for technologies and methodologies acceptable to render PHI unusable, unreadable, or indecipherable to unauthorized persons, then their operations fit within a safe harbor, and they are not required to give the prescribed notification.

Methods of Providing Notice to Individuals

Notice must be provided in writing by first class mail to the affected individuals or by email if the individual has consented to email notification. In circumstances in which there are 10 or more individuals that cannot be reached, a conspicuous posting on the covered entity's Internet home page or notice in major print or broadcast media may serve as a substitute form of notice. If the breach of security has affected 500 or more residents of a state or jurisdiction, notice also must be provided to "prominent media outlets" following the discovery of a breach.

Notice Content Requirements

Notice of a breach of security must include, to the extent possible: (1) a brief description of how the breach occurred; (2) a description of the types of unsecured health information involved; (3) the steps individuals should take to protect themselves from potential harm; and (4) a description of what the entity is doing to investigate the breach, mitigate any losses, and avoid further breaches as well as procedures for individuals to obtain additional information.

Encryption as Method for Securing PHI

Encryption is one of the methods identified for securing electronic PHI from unauthorized access and use. HHS observed that the successful use of encryption depends upon two key features: (1) the strength of the encryption algorithm, and (2) the security of the decryption key or process. The HHS guidance defines acceptable encryption as electronic PHI that is encrypted as specified in the HIPAA security rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key."[5]

The HHS guidance identifies the following encryption processes as having been tested by the National Institute of Standards and Technology (NIST) and judged to meet the above-referenced standard:

- *Data at Rest* — For data that resides in databases, file systems, and other storage methods, the approved encryption processes are those consistent with NIST Special Publication 800-111, "Guide to Storage Encryption Technologies for End User Devices."[6]
- *Data in Motion* — For data that is moving through a network, including wireless transmission, the approved encryption processes are those that comply with requirements of Federal Information Processing Standards (FIPS) 140-2.[7] These include, as appropriate, standards described in NIST Special Publications 800-52, "Guidelines for the Selection and Use of Transport Layer Security Implementations," 800-77, "Guide to IPsec VPNs," or 800-133, "Guide to SSL VPNs," and may include others that are FIPS 140-2 validated.

Destruction

The second methodology identified by HHS to secure PHI is destruction. HHS specified that destruction can occur in one of the following ways:

- *Hard Copy Media* — Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise reconstructed.
- *Electronic Media* — Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, "Guidelines of Media Sanitization" such that the PHI cannot be retrieved.

The HHS guidance is effective upon issuance and applicable to breaches that occur 30 days after publication of the forthcoming interim final regulations.

Submission of Public Comments

The HHS guidance invited covered entities and other interested persons to submit comments on the breach notification rules of the HITECH Act to HHS by May 22, 2009. HHS specifically requested comments on the following:

- Are there particular electronic media configurations that may render PHI unusable, unreadable, or indecipherable to unauthorized individuals, such as a fingerprint protected universal serial bus (USB) drive, which are not sufficiently covered by the above and to which guidance should be specifically addressed?
- With respect to paper PHI, are there additional methods HHS should consider for rendering the information unusable, unreadable, or indecipherable to unauthorized individuals?
- Are there other methods generally HHS should consider for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals?
- Are there circumstances under which the methods discussed above would fail to render information unusable, unreadable, or indecipherable to unauthorized individuals?
- Does the risk of re-identification of a limited data set warrant its exclusion from the list of technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals? Can risk of re-identification be alleviated such that the creation of a limited data set could be added to this guidance?
- In the event of a breach of PHI in limited data set form, are there any administrative or legal concerns about the ability to comply with the breach notification requirements?
- Should future guidance specify which off-the-shelf products, if any, meet the encryption standards identified in this guidance?

In addition to public comment on the guidance, HHS also requested comments concerning any other areas or issues pertinent to the development of its interim final regulations for breach notification. In particular, HHS is interested in comment in the following areas:

- Based on experience in complying with state breach notification laws, are there any potential areas of conflict or other issues HHS should consider in promulgating the federal breach notification requirements?
- Given current obligations under state breach notification laws, do covered entities or business associates anticipate having to send multiple notices to an individual upon discovery of a single breach? Are there circumstances in which the required federal notice also would not satisfy any notice obligations under the state law?
- Considering the methodologies discussed in the guidance, are there any circumstances in which a covered entity or business associate still would be required to notify individuals under state laws of a breach of information that has been rendered secured based on federal requirements?
- The HITECH Act's definition of "breach" provides for a variety of exceptions. To what particular types of circumstances do entities anticipate these exceptions applying?

FTC Guidance for PHR Vendors

Congress mandated under the HITECH Act that the FTC adopt data breach regulations for HIPAA business associates and other entities dealing with PHRs. The HITECH Act also directs the FTC to issue and enforce rules providing interim safeguards and data breach notification requirements for noncovered entities dealing with PHRs. A violation of the FTC proposed rule will be treated as an unfair or deceptive act or practice in violation of the FTC Act.

Security Breach Notification Requirement

On April 20, 2009, the FTC published a proposed rule that would require vendors of PHR and related entities to provide notice to consumers and the FTC when the security of their electronic health information is breached. The FTC proposed rule outlines requirements governing the standard for what triggers the notice, as well as the timing, method, and content of notice.

The proposed rule defines "breach of security" as the acquisition of unsecured PHR identifiable health information of an individual in a PHR without the individual's authorization. A PHR is defined as "an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[8] PHR-related entities include non-HIPAA covered entities "that access information in a personal health record or send information to a personal health record."[9]

PHR vendors are entities, other than covered entities, that offer or maintain a PHR. PHR-related entities are entities, other than covered entities, that offer products or services through the Web site of a PHR vendor or offer products or services through the Web sites of covered entities that offer PHRs to individuals or access information in a PHR or send information to a PHR.[10]

Third-party Service Providers

Third-party service providers are those providing billing or data storage services to vendors of PHRs or PHR-related entities. The proposed rule also stipulates that if a third-party service provider to a PHR vendor experiences a breach, it must notify the PHR vendor, which in turn must notify consumers of the breach. The third-party service provider's notification must identify "each individual" whose information "has been, or is reasonably believed to have been acquired during such breach." The third-party service provider also must provide notice of the breach to a senior official of the vendor or PHR-related vendor and obtain the official's acknowledgement of receiving the notice.[11]

Notification Trigger

"Breach of security" is defined as the acquisition of "unsecured" PHR identifiable health information, as defined in HIPAA: (1) that is provided by or on behalf of the individual, and (2) that identifies the individual or for which there is a reasonable basis to believe that the information can be used to identify the individual.[12] The key requirement triggering the notification requirement is whether the data has been "acquired" and whether the PHR vendor or related entities "reasonably" should have known of the breach through security measures aimed at detecting breaches in a timely manner. The proposed rule presumes that unauthorized persons have acquired information if they have access to it, which can be rebutted "with reliable evidence showing that the information was not or could not reasonably have been acquired."

Timing

The proposed rule requires breach notifications to individuals and the media "without unreasonable delay" and in no case later than 60 calendar days after discovery of the breach. PHR vendors and related entities must provide notice to the FTC "as soon as possible" and in no case later than five business days if the breach involves the unsecured PHR identifiable health information of 500 or more individuals. Breaches involving less than 500 individuals may be accounted for in a breach log and submitted to the FTC on an annual basis from the date of the entity's first breach.[13]

Methods of Providing Notice to Individuals

Notice must be provided in writing by first class mail to the affected individuals or by email if the individual has consented to email notification. In circumstances in which there are 10 or more individuals that cannot be reached, a conspicuous posting on the PHR vendor or related entity's Internet home page or notice in major print or broadcast media may serve as a substitute form of notice. If the breach of security has affected 500 or more residents of a state or jurisdiction, notice also must be provided to "prominent media outlets" following the discovery of a breach.[14]

Notice Content Requirements

Notice of a breach of security must include, to the extent possible: (1) a brief description of how the breach occurred; (2) a description of the types of unsecured health information involved; (3) the steps individuals should take to protect themselves from potential harm; and (4) a description of what the entity is doing to investigation the breach, mitigate any losses, and avoid further breaches as well as procedures for individuals to obtain additional information.[15]

Submission of Public Comments

Interested persons have until June 1, 2009, to review and submit comments on the FTC proposed rule. The FTC rule specifically sought comments on the scope of the requirements and how they related to HIPAA, such as:

- the nature of entities to which its proposed rule would apply;
- the particular products and services they offer;
- the extent to which vendors of PHRs, PHR-related entities, and third-party service providers may be HIPAA-covered entities or business associates of HIPAA-covered entities;
- whether some vendors of PHRs may have a dual role as a business associate of a HIPAA-covered entity and a direct provider of PHRs to the public; and
- circumstances in which such a dual role might lead to consumers receiving multiple breach notices or receiving breach notices from an unexpected entity and whether or how the rule should address such circumstances.

HIPAA Action Items Under the HITECH Act

HIPAA Covered Entities

- Develop a security breach notification process.
- Review and revise business associate agreements.
- Revise accounting of disclosures policies and procedures.

- Revise policies and procedures on the minimum necessary standard.
- Revise policies and procedures on restrictions on disclosures of PHI at the patient's request.
- Revise policies and procedures on marketing using PHI and ensure no sale of PHI or ePHI.
- Develop a methodology to track all disclosures for treatment, payment, and health care operations.
- Audit HIPAA-covered privacy data to ensure all PHI is secure and unsuable, unreadable, or indecipherable.
- Review and update HIPAA privacy and security breach policies and procedures.

HIPAA Business Associates

- Business associates should appoint a compliance officer and comply with applicable HIPAA requirements, including the development of written policies and procedures.
- Business associates should review and revise their business associate agreements.

Conclusion

The HHS guidance provides the means by which covered entities are to determine whether a breach has occurred to which the notification obligations under the HITECH Act and its implementing regulations apply. The FTC guidance implements new breach notification requirements for PHRs. These new HIPAA privacy and security requirements make it imperative that covered entities, business associates, and other entities handling PHRs immediately review and update their data security and privacy practices to guard against growing liability exposures under HIPAA and other federal and state laws.

Covered entities must update policies and practices to avoid these growing liabilities. Business associates that have not done so already also must appoint privacy officers and adopt and implement privacy and data security policies and procedures fully compliant with HIPAA and other applicable federal and state rules.

Endnotes:

1. Office of the Secretary of HHS, "Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposed of the Breach Notification Requirements Under Section 13402 of Title XII (Health Information Technology for Economic and Clinical Health Act) of the American Recovery and Reinvestment Act of 2009.
2. See 74 Fed. Reg. 17914 (April 20, 2009), the proposed rule establishes a new Part 318 of Title 16 of the Code of Federal Regulations for the health breach notification requirement that was mandated by Section 13407 of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5.
3. American Recovery and Reinvestment Act of 2009 at §13402(h)(1)(A).
4. If finalized, the requirement will be found at 16 C.F.R. §318.2(a).
5. 45 C.F.R. §164.304 (definition of "encryption").
6. *See*, National Institute of Standards and Technology Special Publication 800-111.
7. *See*, Federal Information Processing Standards 140-2, which validates certain other standards.
8. See, 74 Fed. Reg. 17914, 17916 (April 20, 2009).
9. Id.
10. Id.
11. Id., if finalized, the requirement will be found at 16 C.F.R. §318.3.
12. Id., if finalized, the requirement will be found at 16 C.F.R. §318.2(a).
13. Id., if finalized, the requirement will be found at 16 C.F.R. §318.4.
14. Id., if finalized, the requirement will be found at 16 C.F.R. 318.5
15. Id., if finalized, the requirement will be found at 16 C.F.R. §318.6

The Evolving Role of Compliance Officers During These Difficult Economic Times

Opportunities for Growth in Compliance are Expanding — Not Diminishing

Paul Belton

Paul Belton is the vice president of corporate compliance at Sharp HealthCare in San Diego, Calif. He can be reached at Paul.Belton@sharp.com.

Fueled by beneficiaries' lack of coverage through job losses and potential Medicaid and Medicare cuts in reimbursement, the financial crisis shared by health care providers has and continues to lead to unprecedented operating decisions. Budget reductions. Hiring freezes. Hospital and clinic closures. Shrinking inpatient admissions. Losses in investments. Higher bad debts due to increase in beneficiary deductible and coinsurance amounts. These are just a few of the difficulties health care organizations, hospitals, and clinics are facing in these turbulent economic times.

Simply put, the current economic crisis has had a significant effect on the supposed recession proof health care industry, but what impact has it had on the health care compliance officer's role? This article highlights some of the realities and potential opportunities the economic crisis is having on the scope and role of the compliance officer in the health care industry.

Weathering the Economic Changes

The economic decline is continuing to ravage the nation's hospitals, with half of them operating in the red and cutting staff. New data show an unprecedented 50 percent of the nation's hospitals appear to be losing money, according to an analysis of government and proprietary data.[1] To date, the results are staggering; 44 percent of hospitals have seen declines in surgeries, with hip procedures showing the steepest drop-off at 45 percent.[2] Even operators of the most robust hospitals are bracing for another difficult year as the effects of layoffs and employer cuts in health insurance benefits take hold.

To add insult to injury, it is not just the recession of the economy itself putting pressure on providers. Pressures are coming from a variety of health care reform initiatives, such as increased external reviews by Medicare recovery audit contractors, Medicaid fraud initiatives, and other third-party payers, causing reduced reimbursement, and rising costs of patient care technologies are forcing organizations to focus on receiving entitled reimbursement.[3]

Ironically, during this economic climate of uncertainty, frustration, and mistrust, the only guarantee is congressional action and new Office of Inspector General (OIG) initiatives, focusing on greater enforcement and greater penalties.

Under the Microscope

Compliance officers need to be aware that compliance initiatives are not given a pass during these difficult times. To make matters worse, compliance department budgets are not revenue generating and may be a conspicuous expense on the balance sheet with no obvious return on investment. As such, compliance officers may be pressured more so than ever before to establish value or produce measurable outcomes and return on investment as part of their compliance program. Perhaps even more alarming is the organization's hidden pressure with employees who may cut corners or take shortcuts with the expectation to maintain productivity or produce greater results.

Despite the need for compliance standards now more than ever, it is often difficult to determine what the "true value" of a compliance program is to an organization. This is often compounded by the fact that the compliance officer may not always be the most popular person in the organization as he or she has the unpleasant task of informing senior management and administration they cannot do things that may be proposed. Consequently, compliance officers have the ability and the duty to uphold the highest possible professional standards and do what they can to restore the public's trust.[4]

A Silver Lining

A compliance officer's ability to prove value to the organization will be critical in the next few years; ironically, however, there is no better time that the health care industry is in greater need of effective compliance actions than in tough economic times. As Security Exchange Commission Director Lori Richards implores, "Now more than ever, companies need to take a long-term view on compliance and realize that their fiduciary responsibility requires a constant commitment to investors. This means sustaining their support for compliance during this economic turmoil and beyond it."[5] Inspector General Daniel Levinson similarly underscored these statements at the 2009 Compliance Institute indicating that now is the most beneficial time to emphasize compliance programs.

Despite a difficult economy, strong companies have leaders who are not afraid to talk about compliance. Evidence continues to surface regarding executive-level decisions to be compliant and ensure ethical decisions are made. Kazuo Inamori, the 77-year-old founder of Kyocera, a Japanese maker of products ranging from cellphones to ceramics with annual revenue close to $13 billion, recently criticized U.S. chief executive offer excesses. Mr. Inamori instead emphasized the need for corporations to seek profits supported by sound ethics and a strong sense of morality. Profits need to be achieved by doing the right thing as a human being.[6]

Compliance officers need to capitalize on the moment and realize that there may never be a better time to be leading the charge in compliance. Now more than ever compliance and ethical decision making should be factored into every business decision.[7]

Return to the Fundamentals

There is a saying that fortunes can be made during the worst of economic times; perhaps the same can be said for the growth of compliance. What better time to infuse the health care industry with the message of a return to core compliance values? During the current economic crisis, compliance officers may need to consider a return to their basic skills and the fundamentals of compliance by ensuring their compliance programs are effective and provide added value.

This may be demonstrated by presenting effective indicators and measurements of identified high-risk areas, surveys on compliance effectiveness, hotline call investigations, and the provision of education and training programs in all aspects of compliance.

Continuing education — whether required or not — should be an important part of every organization's core compliance program. Compliance officers need to stay on top of regulatory, legislative, and technological changes in the industry.

Board education should be concise and updated annually, highlighting the increase in industry regulation and intense oversight focus on efforts to reduce fraud, waste, and abuse. Board meeting agendas should include updates on governmental enforcement actions, risks to the organization, and management's plans to meet these challenges. Trending and performance improvement indicators evidencing compliance program value may be performed at this time.

Visibility and involvement from compliance may be more critical than ever. Compliance officers would be wise to be more visible and assertive by working collaboratively with all members of the organization. One of the best ways to enhance value is to offer resources on related issues, communicate effectively, and attend to problems and issues immediately. The current economic crisis also lends itself the opportunity for compliance officers to show even greater character and honor. During these uncertain times, it is most important to uphold the highest ethical standards when it is most difficult to do so — when the stakes are highest or when cutting ethical corners may be advantageous to employers.

Tremendous Opportunities

A compliance officer's role has never been more opportunistic. Areas of growth, development, and integration are far closer than one may think. Every compliance officer should be prepared to support and seek involvement into a variety of "high-risk" areas or operations. Significant opportunities immediately exist in a variety of areas, including Internal Revenue Service (IRS) matters, Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules, and enterprise risk management.

The new Form 990 represents a major undertaking for the IRS Tax Exempt/Government Entity Division and is the first complete overhaul of the Form 990 in almost 30 years. The IRS is using the new 990 to "catch up with the times" and address a host of issues involving tax-exempt organizations — real and perceived — that have developed since the last major revision.

From a compliance perspective, the instructions for the 2008 Form 990 mean that large organizations (such as hospitals) filing the form likely will encounter more complicated reporting requirements.[8] From an enforcement standpoint, organizations filing the Form 990 likely will experience more transparent reporting than before. As a result, filing organizations must ensure that their operations and financial structures, including executive compensation, are consistent with their exempt purposes.

HIPAA Privacy and Security Rules

The resurgence of HIPAA on a national level creates compliance-related actions that can begin immediately. The American Recovery and Reinvestment Act of 2009 (ARRA)[9] authorizes more than $20 billion in funding and incentives to support the development of a nationwide health information technology (IT) network.

One of ARRA's key goals is to encourage health care providers, through a combination of Medicare payment incentives and penalties, to adopt the use of interoperable electronic health records (EHRs). The law also includes provisions intended to create a framework to support electronic health data interchanges through the development of standards, implementation specifications, and certification criteria for electronically exchanging health information.

Legislators included in ARRA a significant number of provisions intended to strengthen and improve enforcement of the privacy and security rules under HIPAA. Because HIPAA's original privacy rule was adopted by regulation, in most instances the new law amends the regulations, rather than the HIPAA statute.

In any case, however, the new privacy and security provisions will require HIPAA covered entities to modify many of their policies, procedures, and business associate relationships.[10] Moreover, many of these privacy and security provisions in ARRA require the Department of Health and Human Services (HHS) to promulgate regulations explaining specific requirements for covered entities. In some cases, the regulations do not have to be issued for another 18 months. Despite the lag time, some experts say covered entities should begin the compliance process now.

Perhaps the most important modification made by ARRA is a new federal breach notification requirement. The law creates a new definition of "unsecured protected health information" and requires that individuals be notified of any security breaches involving unsecured PHI and, under certain circumstances, that HHS and the media be notified as well. HHS will be responsible for developing breach notification guidelines through regulation.

Compliance officers need to educate their organizations so they understand the elevated importance of privacy and security. Under ARRA's new penalty provisions, there is an increased potential of significant fines being levied, so compliance officers should prepare by readying their organizations for new requirements.[11]

Enterprise Risk Management

In this environment, it is becoming more critical for organizations to find more efficient and proactive means to managing regulatory compliance risks that require early identification and monitoring of all risk areas. As new and rigorous regulatory standards are enforced by new government contractors such as the Medicare administrative contractors, organizations will be forced to adopt compliance risk management identification and monitoring solutions as part of new business strategies and information technology operations.[12]

Addressing these broad concerns may be accomplished through the compliance officer's role expanding into the arena of enterprise risk management (ERM). ERM is the process of planning, organizing, leading, and controlling the activities of an organization to minimize the effects of risk on an organization's capital and earnings. ERM expands the process to include not just risks associated with accidental losses but also financial, strategic, operational, and other risks.

In recent years, external forces have fueled a heightened interest by organizations in ERM. Industry and government regulatory bodies, as well as investors, have begun to scrutinize companies' risk-management policies and procedures. The health care environment now requires significant financial dexterity when handling system risks strategically while encouraging compliance officers to broaden their risk management perspectives and seek organizational alliances outside their core competency or specialty.[13] By taking a proactive approach to risk management using an ERM model, health care organizations and compliance officers will be better equipped to focus on all risk throughout the organization while maintaining patient safety, ensuring compliance, and improving their organization's bottom line.

Shedding Light on Financial Indicators

Although critical, some of the opportunities mentioned above still may not be able to demonstrate a tangible return on investment. Alternatively, another approach compliance officers may consider to expand their role is to underscore financial risk or financial opportunities. A compliance officer's span of influence not only can bring compliance issues imperiously to senior management but in doing so also can highlight a variety of financial indicators.

Looking at the industry's most pressing imperatives — from the perspective of those who face these issues every day — Ernst & Young surveyed the chief executive officers (CEOs) of 19 renowned U.S. provider care organizations nationwide. The number one specific area of concern confronting their hospitals was overcoming financial challenges.[14]

The financial challenges identified by the CEOs included successfully navigating the credit crisis; addressing the impact of reduced reimbursement; providing care to the uninsured and underinsured; coping with bad debt write-offs; accessing capital to grow facilities, successfully navigating the credit crisis, and the prospect of an economic recession; and keeping up with the high cost of unionized nursing.[15]

In addition to these challenges, the OIG is implementing continuously a variety of new areas of investigation to oversee compliance with ever-changing Medicare payment regulations, including reliability of hospital-reported quality data, coding trends, and patterns since implementation of the new Medicare severity diagnosis-related groups (MS-DRGs) specifically looking for potential upcoding and review of hospital compliance with reporting never events, and the Centers for Medicare & Medicaid Services' (CMS') oversight in detecting and preventing payment for medical errors.

Such challenges and concerns present as timely opportunities to compliance officers who may have an open door to engage in revenue cycle management in a wide variety of areas, including revenue integrity, denial management, documentation improvement programs, and recovery audit contractor (RAC) program coordination.

Revenue Integrity and Denial Management Programs

Rejects and denials, underpayments, and unbilled inventories are a threat to the bottom line. Although most hospitals routinely target these functions for improvement efforts, financial success ultimately may depend upon a strong commitment to revenue integrity. Revenue integrity requires that each process in the revenue cycle is performed correctly the first time. It also requires a holistic view of the revenue cycle, one that transcends boundaries around traditional functions and roles, and it requires the timely use of key data.[16]

Compliance officers can assist patient financial services (PFS) departments in identifying systemic patterns of error and facilitating getting information about denials to the personnel who can do something about it. Compliance officers should be members of the denial management team and assist in establishing goals and benchmarks. Compliance staff may be able to enhance the denial management process and facilitate clean claim submission and contribute to reducing days in accounts receivable through their experience in documentation and compliance coding audits.

Most hospitals have some type of *ad hoc* solution in place to try to manage the denial process, but effectively managing denials requires a comprehensive multistep plan involving multiple departments and coordination of each element of the revenue cycle. A robust denial management program includes compliance monitoring and creates point-of-service education improving accuracy and resulting in fewer future denials. The financial impact of denials creates an impetus for a review of the entire system of care, including clinical and operational implications that ultimately benefit both hospital and patient.[17]

Documentation Improvement Programs

Another area of opportunity regarding potential financial compliance initiatives is coordination with clinical documentation improvement programs. Documentation programs continue to evolve in some fashion. Most of these programs are based on the premise that by having inpatient clinical documentation that accurately reflects the severity of patient conditions and acuity of care provided, the accuracy of clinical outcomes, public reporting, and hospital revenue will be improved appropriately. The primary focus is on concurrent processes and physician queries to obtain more specific and detailed documentation.[18]

Internal clinical compliance audits may identify significant opportunity for improvement in administrative data due to the lack of clinical documentation resulting in inaccurate or inadequate coding, patient severity assignment, and reimbursement opportunities. Return on investment can be tracked easily with such a program with some significant team building and cross training between many critical departments.

Recovery Audit Contractors

The CMS permanent RAC audit program presents itself as a new financial compliance risk opportunity. Determining cases at risk, prioritizing the recoupment impact, and performing coding and medical necessity reviews should be spearheaded by a RAC committee. Compliance officers can play a major role in the preparation of the permanent RAC audit program and should be identifying and correcting possible exposure to RAC target areas, reducing overpayment denials, and minimizing payment recoupment.

Pre-RAC audits of targeted claims should be conducted by independent internal or external staff using data mining techniques, coordinated by compliance. Compliance officers also should be prepared to assist their organization in the management and tracking of RAC medical record requests and appeal tracking systems.

In spite of RAC delays, the time period for RAC audit review remains from October 1, 2007, to the current date. Therefore, the delay adds months to the review period, increases the number of claims subject to review, and makes the RAC requests more difficult to handle in a timely manner. Instead of taking a deep breath and deferring the start of RAC preparation, compliance officers and prospective payment system (PPS) hospitals should prepare immediately for the permanent RAC program.[19]

A New Horizon

Finally, one could argue that perhaps the most relevant opportunity to a compliance officer's role lies in quality initiatives and quality of care oversight. With the government's use of data mining technology, nonpayment for hospital-acquired conditions or never events, and other intense review processes, providers must take affirmative steps to address quality of care risks to ensure that they receive all appropriate payments for services and to ensure that they do not run afoul of the fraud and abuse laws leading to enforcement actions.[20]

Even more so, the quality-related health care reform reimbursement proposals being discussed in the U.S. Senate could radically alter health care reimbursement, incentives, and strategy. This, in turn, may alter the role of compliance officers as they relate to quality of care initiatives.

With its significant overhaul of the inpatient prospective payment system (IPPS) and inpatient and outpatient quality reporting measures now in place, CMS is proposing further transformation of its methods of paying hospitals to promote quality and efficient use of resources. CMS has proposed a new quality-reporting program that would cut current Medicare payments to hospitals but would provide incentives if a hospital performed well on a set of quality measures, including 30-day mortality outcomes, clinical processes, and patient significant surveys.

Addressing quality of care proactively, and integrating it with compliance, will place a hospital at a tremendous financial and operational advantage, not only because it will position the hospital to be

Continued on page 64

Achieving Consistency in Your Compliance Program at a Large Multihospital System

Effectively Communicating the "Compliance Message" throughout the Organization is Critical

Gene DeLaddy / Kathryn Dever

How can the chief compliance officer be confident the same message and expectations are being communicated to everyone? If the compliance officer is familiar with the "eighth essential element" of the Office of Inspector General's (OIG's) Compliance Program Guidance for Hospitals, he or she understands the expectation that an effective compliance program should have a culture of compliance, ethics, and integrity that drives decision-making on every level.

The underlying idea is that an organization with a strong *culture of compliance and integrity* consistently and inherently promotes and cultivates compliant and ethical decision-making and good judgment. Implementing this culture, however, will not be achieved through the development of a policy or the creation of a committee; rather, a culture of compliance and ethics is the result of a commitment on the compliance officer's part and the part of every employee to make it an integral piece of everyday operations.

Many compliance officers face the dilemma of implementing or managing a compliance program in a growing organization with multiple facilities that provide a variety of services to residents throughout a large region. These are the challenges that the compliance department team members at Carolinas HealthCare System (CHS), based in Charlotte, North Carolina, manage everyday. CHS owns, leases, or manages 25 hospitals in North and South Carolina and employs more than 40,000 full-time or part-time employees. Additionally, over 1,100 CHS physicians practice in more than 300 locations throughout our facilities.

Gene DeLaddy, CIA, senior vice president, currently serves as the chief compliance officer, chief audit executive, and chief privacy officer of Carolinas HealthCare System, the nation's 3rd largest not-for-profit multihospital system, based in Charlotte, North Carolina. He can be reached at Gene.DeLaddy@CarolinasHealthcare.org or by phone at 704/512-5900.

Kathryn Dever is a director in the Corporate Compliance Department of Carolinas HealthCare System. She serves as the facility compliance director of the system's second largest hospital where she oversees the ongoing auditing and monitoring functions, education, and investigations related to compliance. She can be reached at Kathryn.Thibodeau-Dever@CarolinasHealthcare.org or by phone at 704/512-5927.

As CHS continues to grow, the corporate compliance department, comprised of four focus areas — facility compliance, physician compliance, corporate privacy, and internal audit — must evaluate continuously and refresh the way it does business. Our goal is to ensure the compliance "message" reaches everyone and that the compliance program for each facility is commensurate with its size and complexity. A part of this continuous re-examination involves focusing on five core elements to achieve the goal of systemwide compliance program consistency: board education and reporting, enterprisewide education, ongoing open communication, auditing and monitoring, and evaluation of compliance program effectiveness.

The Board Must Support a Culture of Compliance

The tone at the top is critical for an effective compliance program. The CHS board supports the senior executives' efforts to raise our employees' awareness of the corporate emphasis on ethical conduct and personal integrity. The board looks for consistency of message and information that demonstrates the desire of our employees to implement and achieve the program goals of compliance, ethics, and integrity.

The consistency of message is a product of shared policies, a common code of conduct, consistent employee education, and routine auditing of operations. The compliance officer must routinely educate the board on the functions and importance of the compliance program. A board that has been educated about compliance will ask the right questions and seek to understand the root cause of compliance issues. Furthermore, it will support the compliance officer in his or her efforts to achieve consistency and minimize risk.

Consistency through Education

Just as the board must receive routine compliance education, so should all employees of the organization. It is no surprise that education has become a fundamental element of a strong compliance program. Education can serve as a method of raising awareness, providing real-world experiences, and refreshing workforce members' knowledge about compliance program expectations and requirements.

A key element of any effective compliance program is recognizing that there are numerous ways in which individuals learn. The compliance department must develop a program that can influence and teach *all* levels of the workforce and accommodate all adult learners.

- **Create education that makes an impact.** Utilize recent news stories and events to help make the message more meaningful for all employees. In new employee orientation, use a recent headline news story or event and have audience members identify the compliance issues. Create the opportunity to discuss how your organization conducts its business to avoid situations demonstrated by the case. Use the opportunity to discuss reporting mechanisms and the importance of reporting issues as soon as they are identified.
- **Make education available to everyone**. Education materials and tools are only effective when they are accessible and easy to use.
  - For organizations with teleconferencing capabilities, publicize department-sponsored educational "seminars," develop a registration methodology (for documentation purposes), and broadcast the education session to multiple facilities. For the individuals unable to attend, tape the session and make it conveniently available on your corporate Intranet.
  - Sharing educational materials among facilities is critical. For multihospital systems, encourage compliance representatives to utilize compliance department standard education materials. While minor modification may be required depending on the facility and

types of services provided, encourage as much consistency as possible to ensure all employees are receiving the same message.

- **Use education to raise awareness and evoke a sense of loyalty and commitment to the organization and the compliance program.** Recognize that compliant behavior does not occur just because the organization has a set of policies and procedures available on the Intranet. Compliant behavior results from employee awareness and connection to the mission of the organization and the compliance program, which should be something similar to "doing the right thing." It is important for compliance officers and their teams to find unique and compelling ways to help employees feel committed to doing the right thing, even if the right thing to do in a situation is ask.
  - Use non-health care-related examples and scenarios that draw upon participants' past experiences when they had to employ personal "judgment." Some examples include: Telling a friend's secret to others; speeding up at yellow lights; returning money to a cashier who miscounted at the register.
  - Tie the message of good judgment back to the compliance program to help employees understand the importance of doing the right thing and identifying and reporting instances of noncompliant behavior.
- **Use education in conjunction with disciplinary actions to help diminish the potential for repeated inappropriate activity.** When disciplinary action is used, the employee is frequently told he or she is being sanctioned for "violating policy." It is important for the manager to understand the grounds for the sanctions and to clearly convey those reasons to the employee. Corporate compliance can serve as an educational resource for managers who need to understand how the issue can be prevented in the future.
- **Incorporate compliance education into audit reports to continuously reinforce hot topics and compliance basics for management.** Include regulatory information, references, and descriptions of why the review was completed and what the expectations are for compliance. This will help management better understand compliance expectations and communicate those expectations to their staff.
- **Make the code of conduct the cornerstone of all compliance education and training.** Broadly distribute a universal, systemwide code of conduct. Make this a "living" document that represents the organization's culture of compliance and ethics by referencing it frequently in education sessions. Incorporate elements of all three programs in the code, emphasizing the importance of compliance, privacy, and internal audit to the effectiveness of the compliance program.

By infusing compliance education with creativity and a message, compliance officers and their teams will reap significant rewards. Consistently raising employee awareness about compliance happens when employees are able to take away the "message" of compliance and resources for reporting. The next important step to take is opening the lines of communication to allow employees to feel comfortable asking questions, raising concerns, or requesting additional education.

Consistency through Open Lines of Communication

Education is an effective way of helping raise awareness about the compliance program. In addition to the knowledge of the compliance program, employees also need to feel comfortable communicating with the compliance department about potential compliance concerns. The compliance department is responsible for conveying its "open door policy." It is important to rely on the compliance committees and other workforce members to help get this message out and the work done.

- **Create a network.** The Carolinas HealthCare System Compliance Program Matrix model taps into the involvement of over 450 people across the organization, representing all facilities and identified high-risk functional areas. The privacy program utilizes a similar model to deploy the privacy function. The employees involved in these programs know who their counterparts are at the other facilities and how to get in touch with them. They frequently share best practices and ideas for improvement with one another.
- **Be clear.** Clearly delineate the scope and responsibilities of each program component (on the corporate, risk area-specific, and facility-specific levels) so that everyone knows their role and the resources available to them. Be sure, however, to build in flexibility where areas of overlap exist.
- **Meet often.** Establish a regular schedule for meeting with representatives throughout the organization. Use these meetings to disseminate information on the general compliance environment as well as the organization's internal compliance environment, updates to pertinent laws and regulations, modifications to the program's structure, and valuable opportunities for education and information sharing.
- **Be available.** Promote the use of *ad hoc* interdepartmental communication — pick up the phone to ask questions and share relevant insights. Host a compliance director open forum. Document conversations and advice given to create a database of guidance and decisions. By focusing on making the compliance department approachable and seen as an ally, direct calls and the reporting of potential concerns will increase significantly.
- **Become a hot topic in departmental staff meetings.** Call upon department managers to regularly include compliance or privacy discussion in their departmental staff meetings. Emphasize the importance of documenting attendance and the topics discussed.

When employees consistently hear "the message of compliance," they develop the ability to identify compliance issues and report those issues appropriately. Additionally, management becomes comfortable requesting the advice and guidance of the compliance department staff by seeking out information and, in some cases, requesting audits.

Consistency through Auditing

Auditing and monitoring can be accomplished through a variety of different individuals, including compliance department staff, internal audit staff, compliance risk area representatives, and even front-line managers and staff members. Auditing and monitoring does not have to be overly technical or complicated to be effective. The focus, however, should always be on identifying and understanding risk throughout the organization. Auditing and monitoring must become a fundamental piece of the compliance program. For large multihospital organizations, this can be accomplished a number of ways.

- **Create ways to make auditing and monitoring a part of front-line managers' everyday business.** An advantage of a multihospital system is the opportunity for larger, more established facilities to share tools, knowledge, and best practices with the smaller facilities in the organization. The compliance department must encourage the creation and sharing of tools and templates to support auditing, education, investigation, and documentation. The compliance department can become a clearinghouse for these innovative resources, which can support the goal of consistency throughout the compliance program.
  - Develop common self-monitoring tools and action plans by functional area for use by all entities across the system. Provisions regarding applicability of

each element can be made to accommodate each entity's scope and size, but a shared template of core elements promotes consistency. Additionally, fundamentally similar action plans and self-monitoring allows for comparative trending and consistent corporate reporting of findings across the various facilities within a system.

- **Coordinate auditing work plans and schedules to identify potential areas of overlap or opportunities where knowledge sharing would be beneficial.** Find opportunities to give the internal auditors a chance to identify potential compliance concerns and refer them to the corporate compliance department. Educate compliance auditors about privacy issues and have them look out for potential privacy violations to refer to the appropriate team. Sharing knowledge among auditors within the various departments of the compliance program will increase the opportunity for identifying potential issues in the field.
- **Leverage the organization's size and complexity to identify and manage risk.** Multihospital systems have the unique advantage of being able to identify risk through the findings of internal investigations and external inquiries.
  - If an audit at one hospital identifies significant findings, these results might be an indicator that other facilities in the system are at risk for making the same errors. In these situations, internal findings have indicated risk for the organization. This "risk" can be communicated to the board and the compliance committees and can be managed through appropriate risk assessment, planning, and auditing.
  - Alternatively, if hospitals in the system become the target of a federal or state probe investigation, the compliance officer can use the findings from these external inquiries to understand the compliance risk for the entire organization. Using the focus areas and findings of these inquiries as part of the risk assessment and management process will allow the compliance officer to take a more comprehensive and consistent approach to managing the compliance program throughout the organization. For this approach to work, the compliance department must employ a flexible auditing and monitoring work plan, which can be modified on a monthly or quarterly basis.

The board relies on the reporting that comes from the chief compliance officer. By reporting systemwide trends in audit findings or quarterly monitoring results by facility, the board can get a relatively succinct and accurate snapshot of the organization's compliance program and the compliance risks that it faces. The board also can use this information as a preliminary gauge of the effectiveness of the compliance program.

Encourage Consistency through an Annual Audit of the Compliance Program

While compliance program reporting occurs frequently throughout the year when the board receives its quarterly or semiannual reports, the board and senior management need a good understanding. CHS utilizes internal resources to evaluate the effectiveness of the compliance program.

Annually, the CHS corporate compliance program undergoes a compliance program effectiveness review conducted by the internal audit department. Auditors interview members of compliance committees in each of the facilities throughout the system, requesting detailed documentation of their compliance activities and issues reported to the compliance program.

The report of the annual compliance program effectiveness review is shared with the Finance and Compliance Committee of the board annually. The auditors regularly find opportunities for improvement and areas where the corporate compliance department should provide additional focus in the coming year. The results of the audit and the best practices identified are also shared with all compliance directors, which helps foster consistency and strengthen the compliance program throughout the multiple facilities in the organization.

Plan for the Future

Given the ever-increasing scrutiny on health care providers as a result of numerous new regulations and standards, chief executive officers, under the direction of the board, are asking themselves everyday, "Does every employee in my organization know and understand the importance of compliance? Are we consistently getting the message out?"

The responsibility for the answer rests with the chief compliance officer. Compliance officers of large multihospital systems know they cannot do it alone, so they rely on the support of the board and senior management as well as the compliance department staff, compliance committees, and most importantly, the front-line employees who are responsible for day-to-day operations. Consistency comes from effectively communicating the "compliance message" to everyone throughout the organization to create a unified understanding and a unified purpose.

Long-Term Care Hospitals — the Other Acute Care Setting

Payment Errors Identified through Medicare Medical Review

Kimberly Hrehor / Anita J. Bhatia / Karen Sabharwal

Disclaimer: The analyses upon which this publication is based were performed under Contract Number 500-HHSM-500-2006-TX003C, entitled "Hospital Payment Monitoring Program Quality Improvement Organization Support Center," sponsored by the Centers for Medicare & Medicaid Services, Department of Health & Human Services. The views expressed in this paper are those of the authors and do not necessarily reflect the official position of the Centers for Medicare & Medicaid Services or the U.S. Department of Health and Human Services.

Kimberly Hrehor, MHA, RHIA, FACHE, CHC, and Karen Sabharwal, MPH, are with TMF Health Quality Institute. Kimberly Hrehor was the project director for the Hospital Payment Monitoring Program (HPMP) Quality Improvement Organization Support Center. **Karen Sabharwal** oversaw data analysis activities to support the HPMP. They can be reached at 800/725-9216 or by email at kim.hrehor@tmf.org and ksabharwal@txqio.sdps.org, respectively. **Anita J. Bhatia**, PhD, MPH, is with the Centers for Medicare & Medicaid Services in Baltimore, MD, where she served as the Government Task Leader for the HPMP. She can be reached at 410/786-7236 or by email at anita.bhatia@cms.hhs.gov.

The compliance landscape for long-term care hospitals (LTCHs) is shifting as the possible extent of erroneous Medicare payments to this facility type continues to draw attention. A recent change — the Medicare, Medicaid, and SCHIP Extension Act of 2007 (Public Law No. 110-173, Section 114) signed into law December 29, 2007[1] — requires fiscal intermediaries (FIs) and Medicare administrative contractors (MACs) to review the medical necessity of admissions to LTCHs and continued stays at LTCHs for discharges occurring after October 1, 2007.

These medical necessity reviews are to provide for a statistically valid and representative sample of admissions and guarantee that at least 75 percent of overpayments received by LTCHs for medically unnecessary admissions and continued stays of LTCH patients will be identified and recovered. These reviews also are intended to ensure that related days of care will not be counted toward the length of stay required for LTCHs to retain their Medicare status as an LTCH. The Centers for Medicare & Medicaid Services (CMS), which oversees the FIs and MACs, has the responsibility of implementing these requirements and has begun to do so.[2]

Payments to LTCHs have been the subject of previous compliance investigations.[3,4] In one report, the U.S. Department of Health and Human Services' Office of Inspector General (OIG) identified several potential areas of concern related to LTCHs within a hospital,[3] including incentives for host hospitals and LTCHs within a hospital to discharge and readmit between the two hospitals to receive additional payments — an activity sometimes referred to as "churning." LTCHs are paid under a diagnosis-related group (DRG)-based prospective payment system (PPS) for each admission, so "churning" results in multiple payments between the hospitals involved.

The OIG also examined short stay outliers (SSOs),[5] a billing designation created to provide reduced payment when the LTCH patient has a substantially shorter length of stay than expected for a particular DRG. The SSO threshold is five-sixths of the geometric mean length of stay for the DRG. If a discharge occurs on or before that day, the stay is classified an SSO, and reimbursement can be reduced. The OIG found that SSOs as a percent of LTCH discharges decreased from 40 percent in fiscal year (FY) 2003 to 27 percent in FY 2006. Concomitantly, however, LTCHs increasingly discharged patients within two days after the patients qualified for full long-term care (LTC)-DRG payments, ensuring maximum payment while minimizing length of stay.

LTCHs have continued to interest the OIG; the OIG work plans for 2007 and 2008[6,7] included reviews of LTCH claims for other compliance areas, including appropriateness of payment, admissions from a sole acute care hospital, the 25-day length of stay requirement, and correctness of interrupted stays.

Figure 1: Comparison of Projected Net Dollars in Error by Error Type, Fiscal Years 2005 and 2007

	FY 2005*				FY 2007			
	Original Payment	Net Dollars in Error	Standard Error of Net Dollars in Error	% of Total Net Dollars in Error	Original Payment	Net Dollars in Error	Standard Error of Net Dollars in Error	% of Total Net Dollars in Error
DRG Change	$339,586,224	$ 35,926,152	$11,353,793	14.7	$315,737,403	$ 14,304,542	$12,982,184	10.0
Admission Denial	$197,066,376	$197,066,376	$22,086,780	80.6	$109,721,399	$109,721,399	$15,620,644	76.4
Lack of Documentation	$ 11,417,840	$ 11,417,840	$ 6,435,804	4.7	$ 19,501,556	$ 19,501,556	$11,720,434	13.6
Total	$4,109,737,606	$244,410,367	$25,654,513	100.0	$4,344,516,015	$143,527,497	$23,450,164	100.0
Rate of Improper Payments	5.9 ± 0.6%				3.3 ±0.6%			
Total Discharges**	131,765				132,019			

* FY 2005 is used as the initial year for comparison due to differences in the FY 2004 sampling scheme.[1] Other possible errors are billing errors and Maryland length of stay errors, but none of these error types were found in the sampled claims reviewed. Data as of January 2009.

** Total discharges at the time of sampling.[2]

1. All data in this study were obtained under the Hospital Payment Monitoring Program. Under this program, for FYs 2004-2007, short-term acute care claims were sampled by the date of discharge; long-term acute care claims were sampled by the claims processing date for 2004 and by the date of discharge for FYs 2005-2007.
2. Krushat, W.M and Bhatia, A.J. Estimating Payment Error for Medicare Acute care Inpatient Services. *Health Care Financing Review*, 26(4), 2005.

What is a Long-term Care Hospital?

LTCHs and short-term acute care hospitals (STCHs) are similar in that both types of hospitals admit and treat patients whose medical condition requires an inpatient hospital setting. LTCHs, however, are intended to treat patients with medically complex conditions that require an acute level of care for longer periods than traditionally provided in the STCH setting;[8] acute referring to a high level or intensity of care.

LTCHs typically provide extended medical and rehabilitative care for patients who are clinically complex and suffer from multiple acute or chronic conditions. Services may include comprehensive rehabilitation, respiratory therapy, cancer treatment, head trauma treatment, and wound or pain management.[9]

For Medicare payment purposes, LTCHs are separated from STCHs under section 1886(d)(1)(B)(iv) of the Social Security Act, where LTCHs are defined as having an average inpatient length of stay of greater than 25 days.

New Legislative Requirements

The Medicare, Medicaid, and SCHIP Extension Act of 2007[10] preserved the average length-of-stay requirement for LTCHs and further defined an LTCH as a hospital "primarily engaged in providing inpatient services, by or under the supervision of a physician, to Medicare beneficiaries whose medically complex conditions require a long hospital stay and programs of care provided by a long-term care hospital." New facility criteria requiring LTCHs to have a patient review process that screens patients for appropriateness of admission and validates that the patient meets LTCH admission criteria within 48 hours of admission also were included.

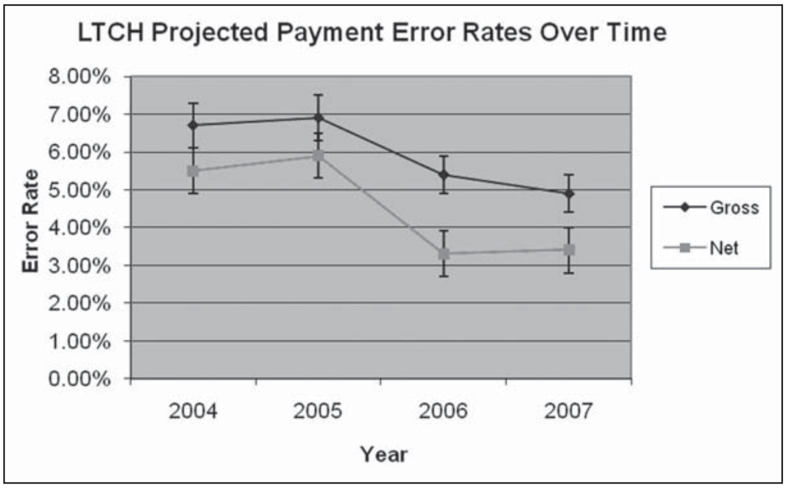
Further, the law states that LTCHs regularly must evaluate their patients' need for continued care and availability of discharge options. LTCHs must have active physician involvement with patient care, including a physician available onsite daily and additional consulting physicians on call. Lastly, LTCHs must have an interdisciplinary team of health care professionals to prepare and carry out an individualized treatment plan for each patient.

Concerns about LTCHs

LTCHs have drawn attention by regulators and other oversight entities due to rapid growth in the number of facilities, annual discharges, and Medicare payments.[11] Medicare is the major payer of LTCH services, and the LTCH prospective payment system is the highest-paying PPS in the Medicare program. Both the PPSs for STCHs and for LTCHs are based upon the same DRGs. The average payment for LTC-DRGs, however, is much higher than the average payment for the same DRG under the PPS for STCHs. Data collected under CMS' charge to estimate an annual Medicare fee-for-service error rate [12,13] found an estimated average payment for LTCH discharges occurring during FYs 2004-2006 of $30,917, compared to $8,078 for STCH claims sampled during the same period.[14]

Until FY 2003, LTCHs were reimbursed under a cost-reimbursement-based system for Medicare payment. Beginning with FY 2003, the payment environment changed

Figure 2: LTCH Claims Payment Error Rates ± Standard Error, FYs 2004 – 2007



when federal regulations published August 30, 2002, established a PPS for Medicare payment of inpatient hospital services furnished by LTCHs.[15]

Under 42 CFR §412.508(a), the medical review oversight of LTCHs was established by stating that a LTCH must have an agreement with a quality improvement organization (QIO) (formerly a peer review organization [PRO]) to have the QIO review on an ongoing basis the following: "(1) The medical necessity, reasonableness, and appropriateness of hospital admissions and discharges. (2) The medical necessity, reasonableness, and appropriateness of inpatient hospital care for which outlier payments are sought under the outlier provisions of §§412.523(d)(1) and 412.525(a). (3) The validity of the hospital's diagnostic and procedural information. (4) The completeness, adequacy, and quality of the services furnished in the hospital. (5) Other medical or other practices with respect to beneficiaries or billing for services furnished to beneficiaries." Note that this payment oversight responsibility recently has transitioned to the FIs and MACs,[16] with QIOs retaining responsibility for other types of reviews, including quality of care reviews.

Results of Sampling Reviews

With the establishment of the LTC-PPS, CMS began reviewing a simple random sample of 116 discharges per month from all reimbursed LTCH claims nationwide. The primary purpose of these reviews was to estimate a payment error rate for LTCH claims, which along with the short-term acute care error rate contributed to the annual "Improper Medicare Fee-for-Service Payments" reports for CMS. Quality of care reviews were conducted as necessary.[17] These data also served as a resource to guide program efforts to reduce improper payments.[18]

Preliminary results of the first LTCH sample reviewed indicated a high admission denial rate of 29 percent;[19] however, as cases completed the full medical review process[20] during the initial year, and as sampling continued through fiscal year 2007, payment error rates and projected net dollars in error decreased, indicating that oversight can be successful in reducing improper Medicare payments (see Figure 1 and Figure 2). Estimated net dollars paid in error, however, were still about $143 million for about 132,000 annual discharges. Note: the net payment error is calculated by subtracting underpayments from overpayments while the gross error rate is calculated by adding the underpayments and overpayments.

The following are major findings[21] derived from full medical review results (see Figure 3 and Figure 4):

- The percentage of cases in error for LTCHs is 50 percent higher than the percentage of cases in error for STCHs.
- The majority of errors in the LTCH setting were for errors in DRG assignment (most often because the principal diagnosis was not the principal reason for the admission or there were other coding errors such as incorrect procedure codes). The rate of DRG changes in LTCHs was more than twice that found in STCHs.
- LTCHs have a higher admission denial rate compared to STCHs, which means that the patient did not require an inpatient level of care *at the time the patient was admitted.* This finding is unexpected, as patients admitted to LTCHs are to have acute, critical, and complex conditions typically requiring longer courses of treatment.
- For net dollars paid in error, admission necessity errors are

Figure 3: Estimated Case Error Rates for LTCH and STCH Claims FYs 2004-2007

Error Type	LTCH Error Claims	Percent of Total LTCH Claims	STCH Error Claims	Percent of Total STCH Claims
DRG Change	47,896	8.7%	1,840,471	4.0%
Admission Denial	33,687	6.1%	2,272,604	5.0%
Lack of Documentation	2,338	0.4%	453,362	1.0%
Total Errors	83,921	15.2%	4,566,437	10.1%
Universe LTCH discharges = 550,790; Universe STCH discharges = 45,924,743				

the source of most improper payments for both STCHs and LTCHs. For both STCHs and LTCHs, an unnecessary admission determination results in recoupment of the entire associated DRG payment.

- Improper payments for DRG changes occur proportionally higher in LTCHs than in STCHs.

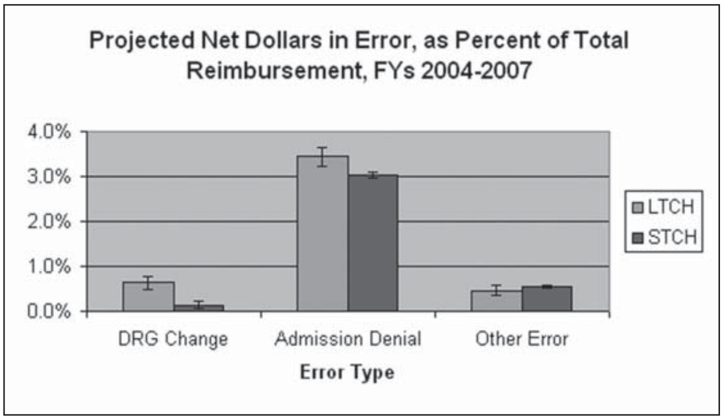
Delving into the claims with errors in DRG assignment revealed that over 20 percent of this subset of claims had the originally billed DRG changed to DRG 462 (Rehabilitation). In addition, for claims with DRG assignment errors, reviewers[22] identified issues related to lack of complete documentation to support the coding of excisional debridement, which is a surgical procedure. A recent *Coding Clinic*[23] has indicated that excisional debridement may be coded if documented as such by the physician. Reviewers found, however, that documentation to support that an excisional debridement was actually performed often was not present in the submitted medical record documentation.

So:

- Why is the admission denial rate higher for LTCHs than STCHs?
- Are there more DRG change errors for LTCH claims than STCH claims because documentation for LTCH claims is not clear as to the reason for the patient's admission or does not support the diagnoses/procedures billed?

At this time, the data can only suggest directions for further research. It is possible that the higher admission denial rate in the LTCH setting could be due to placement of patients in the LTCH who are more suited to other levels of care, such as rehabilitation or skilled nursing care, a hypothesis supported by the incidence of DRG changes to DRG 462. It is also possible that documentation in the medical record simply did not justify the patient's admission, even though there may have been a need. DRG changes could be more prevalent in the LTCH setting due to the relative newness of the LTC-PPS, a hypothesis supported by improvements with oversight.

Figure 4: Projected Net Dollars in Error, as a Percent of Total Reimbursement ± Standard Error, FYs 2004-2007



Suggestions for Compliance Officers

Compliance officers working in the LTCH setting face many of the same challenges as those in other health care settings. As in other settings, collaboration with medical staff, utilization review, and coding staff to examine the hospitals' processes related to compliance issues is critical. It is critical that these individuals work together to:

- ensure that patients require the type and level of care provided by LTCHs;
- closely monitor readmissions from the host hospital (for hospitals within a hospital);
- conduct regular continued-stay review to ensure patients still require an acute level of care; monitor SSOs and patients who are discharged just after the SSO threshold to avoid potential impropriety;
- ensure that documentation contained within the medical record supports the patient's need for admission, the reason the patient was admitted, and all additional diagnoses/procedures;
- follow the Official Guidelines for Coding and Reporting[24] for assignment of the principal diagnosis and when uncertain should query the physician for clarification; and

- review the hospital compliance auditing/monitoring plans to ensure that identified problematic areas are reviewed and any resulting concerns are addressed.

Compliance officers at LTCHs should note the possibility of increased scrutiny and should take steps to ensure compliance programs are sound and maintained; an ounce of prevention is worth a pound of cure!

Additional sources of information about LTCHs include the following:

- Eskildsen, Manuel A. *Long-term Acute Care: A Review of the Literature*. Journal of the American Geriatrics Society. May, 2007. 55(5):775-779.
- Gage, B; Pilkauskas, N; Dalton, K; Constantine, R; Leung, M; Hoover, S; Green, J. *Long-term Care Hospital Payment System Monitoring and Evaluation*. RTI International. January 2007.
- Liu, Korbin; Baseggio, Cristina; Wissoker, Douglas; Maxwell, Stephanie; Haley, Jennifer; Long, Sharon. *Long-term Care Hospitals Under Medicare: Facility-Level Characteristics*. Health Care Financing Review. Winter 2001. 23(2):1-18.
- Medicare Payment Advisory Committee. *A Data Book: Healthcare spending and the Medicare Program*. June 2006.
- CMS Transmittal 1547, CR 6114, July 3, 2008, Update-Long-term Care Hospital (LTCH) PPS FY 2009.

Endnotes:

1. 110th Congress United States of America. Medicare, Medicaid, and SCHIP Extension Act of 2007. Public Law No. 110-173, Section 114. December 29, 2007.
2. American Hospital Association. CMS awards contracts for LTCH medical necessity reviews. *AHANewsNow.* December 22, 2008. Internet address: www.ahanews.com/ahanews_app/searchNewsNow.jsp?date=12/22/2008 (accessed January 5, 2009).
3. Department of Health and Human Services, Office Inspector General, *Long-term Care Hospitals-Within-Hospitals* (OEI-01-02-00630). July 2004.
4. Department of Health and Human Services Office of Inspector General. *Long-term Care Hospitals Short-Stay Outliers* (OEI-01-07-00290). March 21, 2008.
5. Department of Health and Human Services Office of Inspector General. *Long-term Care Hospitals Short-Stay Outliers* (OEI-01-07-00290). March 21, 2008.
6. Department of Health and Human Services Office of Inspector General. *Work Plan Fiscal Year 2007*.
7. Department of Health and Human Services Office of Inspector General. *Work Plan Fiscal Year 2008*.
8. Gage, B., Bartosch, W., and Green, J. *Long-term Care Hospital Project Approach*. RTI International. February 2005.
9. Medicare Payment Advisory Committee. *Medicare Payment Policy*. Report to Congress. March 1999.
10. 110th Congress United States of America. Medicare, Medicaid, and SCHIP Extension Act of 2007. Public Law No. 110-173, Section 114. December 29, 2007.
11. Medicare Payment Advisory Committee. *New Approaches in Medicare*. Report to Congress. June 2004.
12. Krushat, W.M and Bhatia, A.J. Estimating Payment Error for Medicare Acute care Inpatient Services. *Health Care Financing Review*, 26(4), 2005.
13. The CERT reports are accessible at www.cms.hhs.gov/CERT.
14. All data in this study were obtained under the Hospital Payment Monitoring Program. Under this program, for FYs 2004-2007, short-term acute care claims were sampled by the date of discharge; long-term acute care claims were sampled by the claims processing date for 2004 and by the date of discharge for FYs 2005-2007.
15. Federal Register, vol. 67, No. 169. August 30, 2002, pages 55955-56090.
16. CMS Transmittal 264, CR 5849, August 7, 2008, Pub 100-08 Medicare Program Integrity.
17. The CERT reports are accessible at www.cms.hhs.gov/CERT.
18. Bhatia, A.J., Blackstock, S., Nelson, R., and Ng, T. Evolution of Quality Review Programs for Medicare: Quality Assurance to Quality Improvement. *Health Care Financing Review*, 22(1), 2000. The Hospital Payment Monitoring Program (HPMP) was initially implemented as the Payment Error Prevention Program for inpatient PPS services reimbursed under Medicare. The purpose of these programs was to measure, monitor, and reduce the incidence of inpatient PPS improper payments. When the PPS for LTCHs was implemented with medical review under the purview of QIOs, these services came under the purview of the HPMP.
19. In June 2004, CMS held a hospital payment monitoring conference for QIOs. The 29 percent denial rate for long-term acute care claims was based upon preliminary data and was reported at this conference by the CMS Government Task Leader for the program. Subsequently, this preliminary value was reported by Votto, J. National Association of Long-Term Hospitals, 2005. Written testimony before the Committee on Ways and Means, Subcommittee on Health, U.S. House of Representatives. 109th Congress, 1st session, June 16, cited by Medicare Payment Advisory Committee. *Medicare Payment Policy*. Report to Congress. March 2006, cited by

Continued on page 64

The Core of Clinical Documentation Improvement: Physician Documentation Education

Programs Must Be Two-Pronged and Focus on General *and* Specialty-Specific Documentation

Betty B. Bibbins

This article is the final in a series of three articles that discuss why acute care hospital-based clinical documentation improvement (CDI) programs are an important component for compliance, especially with the implementation of the Centers for Medicare & Medicaid Services (CMS) Recovery Audit Contractor (RAC) Program that is now "rolling" into effect across the United States.

In the first article, we discussed why the RAC program was implemented and why CDI programs can proactively support appropriate documentation (and associated coding) of patient care provided. The second article discussed the importance of compliance officers proactively assisting with accountability and regulatory oversight regarding the documentation/medical necessity conditions of participation with Medicare in supporting efforts of acute care facilities with regard to appropriate standards being communicated to Medicare and other third-party payers.

This third and final entry of the series aims to go toward the center of all the other components. While we discuss the appropriate workings of compliance officers, the appropriateness of CDI specialists and coder queries, the medical necessity reviews by utilization review specialists, and the correct billings by revenue cycle specialists, rarely do we see discussions regarding the core of what all of these areas are based upon...physician documentation — more specifically, physician documentation compliance education and documentation of medical necessity.

As physicians, we learn to practice and communicate the practice of clinical medicine physician-to-physician.

Betty B. Bibbins, MD, CHC, C-CDI, CPEHR, CPHIT, is president and chief medical officer at DocuComp LLC. She can be reached at 740/968-0472 or by email at BibbinsMD@DocuCompLLC.com.

In other words, when one physician documents (even in brief medical record clinical entries) regarding patient care, we understand the "short hand" of clinical medicine, thanks to the seven to 15 years of medical training received. We understand the entire pathological continuum process of any given disease process, and we do not necessarily have to write a textbook type of entry for other physicians to understand what we are doing with our patient care.

There is one area, however, that we as physicians receive scant education, and that is regarding documentation for communicating to nonphysician health care providers and meeting criteria for third-party payers — specifically Medicare's conditions of participation for physicians and hospitals that are dependent on physician documentation as the basis for all inpatient and outpatient care provided at their facilities. Medicare's standards are also being utilized by other third-party payers when their methods have been proven to reduce costs and reimbursements for poor quality care and waste within health care.

At this time, we are going to discuss the importance of physician education regarding documentation improvement and how important it is that the hospitals and compliance officers work together to do their due diligence in enhancing physician documentation improvement education in addition to providing support personnel (such as CDI personnel, utilization review (UR) reviewers, coders, and fiscal revenue cycle personnel) that are being utilized already. Without physician whole-hearted cooperation, however, that is based upon appropriate documentation knowledge and education above and beyond medical knowledge, there will continue to be "target rich areas" for RAC data mining recoupment within the medical records of hospitals and physician offices.

Without documentation education being an additional component of a physician's medical education, there will be little forward movement in the areas of compliance. All that can be done is that facilities will work with whatever information they have to work with within the medical record, but it will be only a fraction of the capture of the true severity-of-illness to justify the consumption-of-resources and establish medical necessity for levels of care provided.

Physicians are very good at communicating physician-to-physician. There needs to be additional training, physician-to-physician, through hospital formal, educational medical staff meetings. This training must be two pronged: (1) general documentation education language that all providers must be fluent in; and (2) specialty-specific departmental training for the major areas of medicine and surgery as well as subspecialties such as cardiology, pulmonology, nephrology, and geriatrics. For example, helping physicians communicate in the medical record that patients may have "chronic, stable" comorbid medical problems rather than "past history" of a medical problem.

Patients on long-term medical management may not have had an acute case of a disease process recently, but if the patient becomes ill with another medical problem, or stops taking his or her routine medications, then that specific "past" problem possibly may become an acute, current problem. For instance, a well-controlled diabetic may become an uncontrolled diabetic if a serious infection develops.

Physicians need ongoing clinical documentation education. Acute-care hospitals must make physician documentation education a number one goal to improve the capture of quality of care provided at their facilities and not just clinical documentation improvement support (such as CDI personnel, et cetera) but providing the actual education and updating for physicians.

One route is to work actively to make this education criterion for re-credentialing for medical staff privileges. This will impress upon physicians the true importance of documentation. Also, it will demonstrate that the facility is taking this proactive step in preparation for, and response to, the RACs, Comprehensive Error Rate Testing (CERT) program, Medicare administrative contractors (MACS), and other regulatory agencies that are doing *their* due diligence in actively recovering reimbursements for care quality that is poorly documented, or not documented at all, within the medical record.

One of the main complaints from physicians (from personal experience) is that they know how to document — it has gotten them "this far" in their professional lives — but how many receive feedback in the form of quarterly reports from facilities regarding standards of care goals or core measure goals? Do they have rankings of appropriate criteria for inpatient versus outpatient observation admission criteria? (Individual physician identities are protected, of course.) How many receive any facility feedback, other than the number of queries made of them, and how many do they respond to versus ignore?

Physicians may not know the perceived quality, or lack of quality, that is dependent upon the specificity and completeness of their documentation. They need to know how their profiles as well as the facility's profile are impacted by clinical and medical necessity documentation. This information needs to be communicated to physicians through the medical (*e.g.*, medical staff director, vice president of medical affairs) and administration leadership. This communicates the importance and need for all in health care to work together. Also, the information communicated needs to emphasize that improved documentation means not merely more words within the medical record but more efficient wording within the medical record.

Physicians need to be aware of the compliance components of their practice of medicine as well as the *documentation* of their practice of medicine. This compliance also will help the physician within the proactive aspects of care. It will demonstrate the additional compliance education undertaken by the physician, which also will demonstrate quality of care for which the RACs are searching.

When Medicare went to value-based purchasing, this became the key mechanism for transforming Medicare from a passive payer to an active payer. The current Medicare physician reimbursement schedule is now based upon quantity and resources consumed, *not* on quality or value of services. Thus, to quantify the care provided, Medicare developed the follow equation:[1]

Value = Quality/Cost:
Quality → Quantifiable through outcome studies (claims data analysis and processing from documentation and coding).
Cost → Directly quantifiable through claims data.

To physicians and hospitals, this means that the documentation and coding of care provided, as well as fiscal cost data that are submitted to Medicare (in the health care providers own "words"), are the components used to show the quality and value of care provided. This means that the greater the severity-of-illness managed at the most justifiable cost equates to a better value and higher quality of health care provided. Physicians must know the expectations of documentation of care to maintain and keep our health care system viable in the era of economic decline; we must provide the best levels of care for all severities of illness.

This leads us to a number of questions that we have to ask regarding the capturing of the true levels of care provided to hospitalized patients. These include:

- Does the acute care facility provide annual, ongoing clinical documentation CME (continuing medical education) to attending physicians as a criterion for maintaining active medical staff membership? This could show due diligence on the hospital's part to the improvement of quality as well as the emphasis on compliance for the RACs. This also could include evaluation and management (E&M) documentation education and coding, which would impact physician "buy-in."
- Have your CDI and educational programs been rolled out to physicians by

your hospital leadership to emphasize the importance to the highest levels?

- Do you provide ongoing documentation and medical necessity education for your emergency department physicians? This education can significantly impact the survival of this critically utilized department in today's economic environment.

Clinical documentation education and programs are becoming a major component within acute care hospitals. This is an evolving, new arena within health care by which hospitals and physicians are graded and compared to other providers, regionally and nationally. Programs, including the RACs, MACs, and CERTS, are all ready to judge compliance to Medicare regulatory rules, as well as to recoup past, current, and future reimbursements. Hospitals and physicians are evolving together in ways that shift the paradigm regarding the communication of patient care. Improved communications of compliance and quality of health care will come with these new changes.

Endnotes:

1. CMS VBP White Paper (2007), www.cms.hhs.gov/AcuteInpatientPPS/downloads/hospital_VBP_plan_issues_paper.pdf. Additional information about CMS and the OIG is available at www.cms.hhs.gov, www.cms.hhs.gov/HospitalAcqCond, and www.oig.hhs.gov.

Roy Snell

Former FBI Special Agent Talks about His Move to the "Other Side" of Compliance

Gaining the Respect of Those in Your Organization is Vital to Achieving Success

Matthew F. Tormey is the vice president of Compliance, Internal Audit, and Security for Health Management Associates. He can be reached at 239/552-3503 or be email at Matt.Tormey@hma.com.

Snell: Tell us about your background prior to becoming a compliance officer.

Tormey: I graduated law school in 1990 and practiced law until I was accepted into the Federal Bureau of Investigation (FBI) in July 1991. After attending training in Quantico, Virginia, I was assigned to the New York field office where I worked until December 31, 1999. In January 2000, I left the FBI and joined Health Management Associates as the corporate compliance officer.

Snell: Tell us about your time in compliance and how is it different from your time in the FBI.

Tormey: The most significant difference relates to the scope of responsibilities and the nature of the work. As a special agent with the FBI, my primary responsibility was to conduct investigations. As a corporate compliance officer, I am charged with the responsibility of *implementing*, *operating*, and *monitoring* all aspects of a compliance program, and investigations are just one small part.

Snell: You have mentioned that gaining respect is a key to any compliance officer's success. Can you tell us why it is important and how you have worked to gain the respect of your organization?

Tormey: If your coworkers trust and respect you, they will be more likely to bring concerns to your attention sooner rather than later, they will be more likely to speak up when they suspect illegal, unethical, or otherwise inappropriate conduct, and they will be more likely to fully cooperate during investigations. I know that they are supposed to do those things anyway, but the reality is that it does not always happen. Building relationships based upon trust and respect increases the likelihood that potential issues will be reported and increases the likelihood that a compliance officer will get the call saying "just in case you have not heard…" rather than, "oh, I thought that someone else would have reported this."

The way that I have tried to build these relationships of trust and respect is informally interacting with as many employees as possible at all levels of the company and responding to their questions and concerns. It is no secret that if the compliance officer shows up to speak with an employee, there is a natural reaction for employees to be nervous, concerned, or possibly intimidated. If your first interaction with others is more social than formal compliance business, this helps to break down any barriers to open future communications.

Snell: What are some of the key issues you will be focusing on in the next year?

Tormey: My number one focus area has always been to establish and maintain a culture whereby employees will not tolerate illegal, unethical, or otherwise inappropriate conduct. Two critical elements of this focus area are making employees aware of the risk areas and making them feel comfortable about communicating concerns. In furtherance of this goal, I regularly communicate with all relevant employees about settlements, investigations, audits, and other problematic areas identified by the government.

Snell: You have set up a meeting with some of your former colleagues at the FBI. Tell us a little about the purpose of the meeting.

Tormey: Approximately two years ago, the FBI established an Office of Integrity and Compliance, which is essentially the FBI's internal compliance program. Recently, I helped set up a meeting with representatives from the FBI as well as several compliance experts from different industries to share best practices. The meeting was incredibly productive due primarily to the open and candid discussions by everyone involved.

Snell: You have recently joined the Health Care Compliance Association (HCCA) board. Tell us a little about why you became involved.

Tormey: HCCA is an invaluable resource to thousands of compliance officers throughout the country, and its continued presence and growth is vital. I have benefited immensely from being a member, and now I would like to give the benefit of my experiences back to the organization that has given so much to me and my hospital compliance officers.

Snell: You work with hospitals of all sizes, but some of the hospitals you work with are small and have fewer resources. How do small hospitals deal with the requirement of naming a compliance officer? How do they do it when they have so few resources to begin with?

Tormey: The corporate office has built the infrastructure and provided the resources for all of our hospitals to establish and maintain a compliance program. The hospital compliance officer is designated and trained by the corporate office consistent with the requirements of our compliance program. When there are issues or matters that the hospital compliance officer or other staff do not have the time, expertise, or resources to handle, they will solicit the as-

Continued on page 65

Bob Brown

New Technologies Have Created New Threats to Electronic Protected Health Information

ARRA Privacy Provisions Are Designed to Mitigate These Threats

Bob Brown, PhD, is the director of Health Information Technology, Michigan State University Kalamazoo Center for Medical Studies.

The new privacy provisions contained in the American Recovery and Reinvestment Act (ARRA) have provoked considerable discussion and triggered some dismay. While many of the provisions may appear to present compliance challenges to covered entities, detailed compliance cannot be mapped out yet.

The Act calls for the promulgation of a number of rules, recommendations, and guidance documents from various federal agencies, departments, and committees that will provide the specific details required for compliance. (For a timeline of when these various documents are supposed to be available, go to geekdoctor.blogspot.com/2009/03/timeline-for-arra-privacy-provisions.html). While we are waiting for these documents, it might be instructive to review the rationale behind the new rules. Presumably, this same rationale will guide the forthcoming recommendations, rules, and guidance documents.

Like the original Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules, the new provisions are intended to provide the necessary privacy and security framework that will allow for the continued application of information technologies to help achieve the main goal of the administrative simplification provisions of HIPAA: to improve the efficiency and effectiveness of the health care system. The introduction of the new provisions are designed to address new threats and opportunities presented by new technologies such as interoperable electronic health records (EHRs), personal health records (PHRs), health information exchanges (HIEs), and state and national health information networks (HINs).

Since the adoption of the privacy and security rules, more protected health information is being stored in

EHRs, more individuals are entering their own health information into PHRs, and more of this information is being stored in repositories in HIEs and transmitted through HINs. Many of the organizations operating PHRs, HIEs, HINs, and other systems that are being used to collect, store, and communicate individually identifiable health information are business associates and not covered entities under HIPAA. As such, they were not subject to the enforcement provisions in the HIPAA rules.

ARRA corrects this in section 13401, "Application of security provisions and penalties to business associates of covered entities." Business associates are now directly covered by the HIPAA rules. This section also makes it clear that pretty much any entity that owns or operates any of the components of the emerging health information network in which individually identifiable health information is housed is a business associate.

As more and more individually identifiable health information is transmitted to health information exchanges, stored in online registries and databanks, and transferred from one system to another, more large scale breaches of security are likely. ARRA section 13402, "Notification in the case of breach," is designed to mitigate that risk.

This section mitigates the risk in two important ways. First, it requires notification of each individual whose protected health information has been, or is reasonably believed to have been, illegally accessed, acquired, or disclosed so the individuals can take whatever steps they can to protect themselves. Second, because the notification of breach is only required if the information is unsecured, this rule encourages the use of appropriate technologies to secure protected health information contained in these systems.

Until now, vendors and users of health information technology (HIT) systems have been slow to adopt readily available security technologies that can provide significantly improved protection to PHI in transit and at rest. Many recent high-profile breaches could have been prevented by encrypting data stored on hard drives and portable media.

This new rule should stimulate demand by customers for HIT vendors to incorporate the "technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals"[1] that will obviate the breach reporting requirement even if a hacker is able to penetrate perimeter defenses and get to the data.

In the original HIPAA rules, individuals had a right to an accounting of disclosures of their PHI subject to certain exceptions. One of those exceptions was for disclosures "to carry out treatment, payment and health care operations."[2] Two of the reasons for excluding these types of disclosures from the accounting were the administrative burden of tracking such disclosures as well as the assumption that most disclosures for treatment, payment, and health care operations were of a type that a patient would reasonably expect and anticipate in the normal course of receiving health care.

The accounting was primarily designed to provide the individual with information on those out-of-the-ordinary disclosures of which he or she likely would not be aware. With the increasing amount of PHI online, however, information is being disclosed for treatment, payment, and health care operations in new ways that most patients may not expect (*e.g.,* quality reporting initiatives, disease management, incentive bonuses, et cetera). Also, technology embedded in electronic health records can now automate the process of tracking who has accessed health care records and where electronic information has been sent.

Consequently, section 13405 (c), "Accounting of certain protected health information disclosures required if covered entity uses electronic health record," removes treatment, payment, and health care operations from the list of exceptions to the ac-

Continued on page 65

Rebecca C. Fayed

The Narrowing of the OIG's Self-Disclosure Protocol: Where Do We Go Now?

Rebecca C. Fayed is an attorney in the Health Care Group at Sonnenschein Nath & Rosenthal LLP. She can be reached at 202/408-6351 or by email at rcfayed@sonnenschein.com.

The Ability of Medicare Contractors to Analyze Stark Law Matters Is Unclear

On March 24, 2009, the U.S. Department of Health and Human Services Office of Inspector General (OIG) issued *An Open Letter to Health Care Providers* (the "2009 Open Letter") refining the agency's provider self-disclosure protocol (SDP).[1] The SDP was developed and implemented in 1998 to encourage providers to work openly and cooperatively with the OIG by voluntarily self-disclosing matters involving potential health care fraud.

Although in recent years the OIG has promoted the SDP as a means to resolve matters giving rise to civil monetary penalties (CMPs) under both the federal physician self-referral law (Stark law) and the federal health care program anti-kickback statute, the 2009 Open Letter narrows the scope of the SDP with regard to the Stark law in an effort "to focus [OIG's] resources on kickbacks intended to induce or reward a physician's referral." Consequently, many providers are left wondering: where do we go now if we uncover a potential Stark law violation absent evidence of a kickback intended to induce a referral? The short answer is this: it's not clear.

History of the SDP

The SDP was created in 1998 to "offer health care providers specific steps...that may be undertaken if they wish to work openly and cooperatively with [the OIG] to efficiently quantify a particular problem and, ultimately, promote a higher level of ethical and lawful conduct throughout the health care industry."[2] Stressing the role of health care providers in fighting health care fraud and abuse, the OIG developed the SDP on the premise that health care providers should police themselves, identify potential issues, and work with the OIG to correct and resolve any problems.

To assist providers with this, the OIG developed detailed guidance in the form of a disclosure protocol that includes guidelines for the voluntary disclosure submission, an internal investigation, and a provider self-assessment. The SDP identifies the "basic information" that must be included in the provider's initial submission to the OIG and the "substantive information" that must be included in the report following the provider's internal investigation and self-assessment. The basic information that must be included in a provider's initial submission to the OIG generally includes the following:

- specific provider-identifying information, including name, address, and identification numbers;
- a statement regarding whether the provider has knowledge that the matter being disclosed, or any other matter, is being investigated by the government;
- a full and specific description of the nature of the matter being disclosed;
- the type of health care provider implicated and the federal health care programs affected;
- the reasons why the provider believes that a violation of law has occurred; and
- a certification that the submission contains truthful information and is based on a good faith effort to resolve any liabilities to the government.[3]

In an effort to encourage more providers to utilize the SDP, on April 24, 2006, the OIG issued an *Open Letter to Providers* regarding the SDP (the "2006 Open Letter"). The 2006 Open Letter sought to encourage providers to self-disclose matters by committing to resolve disclosed matters for amounts at the lower end of the damages spectrum, including (as appropriate) a multiplier of the excess benefit conferred on the referral source, as opposed to statutory damages. The 2006 Open Letter also explained that the OIG would consider the disclosing provider's existing compliance program when determining whether a corporate integrity agreement (CIA) or a certificate of compliance agreement (CCA) would be required to resolve the matter.

Presumably, the promise of lower penalties and less onerous integrity obligations was successful at increasing the utilization of the SDP because on April 15, 2008, the OIG issued another *Open Letter to Health Care Providers* (the "2008 Open Letter") announcing clarifications and refinements to the SDP. According to Inspector General Levinson, the refinements and clarifications set forth in the 2008 Open Letter were intended to "increase the efficiency of the SDP and benefit providers who self-disclose."

Pursuant to the 2008 Open Letter, a provider's initial submission under the SDP was required to contain not only the basic information set forth above but also (1) a complete description of the conduct being disclosed, (2) a description of the provider's internal investigation (or a commitment regarding when it will be completed), (3) an estimate of the damages to the federal health care programs and the methodology used to reach that estimate (or a commitment regarding when the provider will complete such estimate), and (4) a statement of the laws potentially violated by the conduct at issue. The Open Letter also stated that each provider must be in a position to complete its investigation and damages assessment within three months of the provider's acceptance into the SDP program by the OIG.

The 2008 Open Letter also reiterated certain issues that the OIG had addressed previously. For example, it stated that the OIG expected full cooperation from disclosing providers and would remove from SDP participation any provider that did not cooperate fully with the OIG in the SDP process. In addition, although the 2008 Open Letter explained that the OIG had streamlined its own internal process for resolving these cases promptly, it also stressed that the efficiency of the process depended on health care providers' determination that the matter constituted fraud, not "merely an overpayment."

According to the OIG, the SDP is appropriate only for matters constituting poten-

Continued on page 66

Matthew Haddad

Continuous Credentials Monitoring: Building a Solid Compliance Infrastructure

Through A Shared Access Platform, Facilities Can Check Status, Generate Reports, and Create Web-based Features

At one time, credentials compliance was only a periodic concern. Every two or three years — depending on whether facilities were accredited by the Joint Commission or the National Committee for Quality Assurance — provider credentials were checked for compliance with quality standards. Today, credentials verification is being performed more often to comply with a host of new requirements related to health care quality concerns.

New Trends in Practitioner Credentials Compliance

Managed Care

As health care organizations respond to the growing trend of consumerism in medicine, physician credentialing processes are likely to change to bring more value to patients and consumers. Ongoing credentialing of physicians is expected to ensure that only high-performing doctors are included in network offerings, with consumers flexing their newly acquired muscles to select a provider that best meets individual expectations.

Most health plans believe that credentialing of physicians has become a value-negative burden to the system, with a growing sentiment that consumers should not be penalized through higher premiums to support a process that is not of significant benefit. According to Derek van Amerongen, chief medical officer of Humana of Ohio, "As the wave of consumerism in medicine continues to build, we must be ready to jettison the outmoded tasks that no longer help consumers but, instead, diminish the return on the resources they devote to health care."[1]

Matthew Haddad is the president and chief executive officer of Medversant, LLC. Medversant provides continuously monitored Web-based credentials verification solutions through patented AutoVerifi^{TM} technology (U.S. Patent 7,529,682) for hospitals, health insurance plans, nursing homes, outpatient centers, and other health care settings. Medversant can be reached at 213/291-6139 or www.medversant.com.

Hospitals

Joint Commission credentialing and privileging standards require that health care facilities no longer conclude that a practitioner's license and privileges are valid in an environment of nonreporting. The new standards are designed specifically to encourage a more evidence-based process.

Hospitals now must factor *continuous practice evaluation information* into decisions to revise, revoke, or renew existing privileges. This entails developing clearly defined, continuous evaluation processes for monitoring clinical practice and professional behavior. Although the type of data collected in the continuous evaluation process would be determined by the organization and approved by the medical staff, relevant data may include:

- operative and other clinical procedure outcomes;
- length of stay patterns;
- mortality rates;
- risk management data; and
- a practitioner's use of consultants, pharmaceuticals, and other treatment modalities.

While there is no specific mandate for continuous monitoring of background information (such as licenses, malpractice coverage, and other documentation), these issues can indicate overall and operative practitioner performance, procedure outcomes, risk management, mortality rates, and other indices. Furthermore, regardless of current accreditation standards, advancements in technology likely impact what may be considered a prudent standard of care.

Ongoing monitoring would seem to go along with achieving the overall goals outlined by the Joint Commission. Arguably, with the technology available, a continuous monitoring program is reasonable and could become the industry standard. Risk managers for hospitals, health plans, Joint Commission-covered entities, or other health care organizations may be well-advised to pursue this level of scrutiny.

Ambulatory Surgery Centers

Furthermore, as the Centers for Medicare & Medicaid Services (CMS) embarks on significant changes to its rules concerning ambulatory surgical centers (ASCs), there is heightened need among ASCs for ongoing monitoring of physician credentials. The proposed rules, widely regarded as the largest change in ASC rules since 1982, cover a wide range of operating issues. If approved, these changes are likely to have a substantial impact on the ASC industry.

New regulations would create a more comprehensive quality assessment and performance improvement program for ASCs, further pressuring these centers to be vigilant about credentialing. Prudent risk management would suggest that ASCs establish a plan to implement the technology that will result in more accurate and up-to-date records at vastly reduced costs. To do nothing risks lower reimbursements, back charges, potential fines, and tort claims asserting negligent credentialing.

ASCs exist in all 50 states and can be found throughout the world. In the United States, most ASCs are licensed, certified by Medicare, and accredited by one of the major health care accrediting organizations. While these surgery centers have always qualified for Medicare reimbursement, the regulatory change impacts reimbursement methodology.

Of special concern is the manner in which the rules will impact the way in which ASCs disclose physicians' financial interests in the facility. Documenting and validating all provider information will be imperatives for compliance and operations within the proposed guidelines.

Additionally, the recently introduced recovery audit contractor (RAC) initiative establishes a Medicare auditing program that utilizes private firms to examine physician, hospital, nursing home, and other health care facility claims to find instances in which the government has overpaid providers. Medicare will deny claims and reimbursement for services when findings uncover, among other things, unlicensed providers.

Health care organizations need to anticipate increases in denials of claims/reimbursement and back charges by aggressive RAC agents for services performed by practitioners with license issues. Currently, most health plans and hospitals only fully verify credentials every two to three years. While CMS does require licenses to be checked at expiration in acute care, the tedious nature of performing these verifications may cause it to be performed in an inconsistent or less-than-thorough manner.

Also, CMS requires that monthly verifications be performed on federal sanctions on providers to ensure that practitioners accepting federal reimbursements are eligible by not having federal sanctions. The process of manually reverifying all practitioners each month is labor-intensive, tedious, and not as accurate as an automated process that obtains the information directly from the applicable databases continuously and reports changes in status to the credentialing staff.

Continuous monitoring and verification of credentials presents a dependable, cost-efficient solution for all stakeholders. Not only will it result in the rapid identification of noncompliance, but continuous monitoring technology encourages greater compliance and diligence by providers, the byproduct of which is "best practices" and reduced risk for the organization as a whole.

Achieving Continuous Data Integrity the Cost-Efficient Way

As a stop gap, organizations may try to continuously monitor their practitioners through manual processes. Staff would be charged with verifying licenses, certifications, and other credentials by provider on a repeating schedule such as once a week, month, or three months, et cetera. This task would include using the Web to search third-party databases, obtain copies of the results found, and then compare the information obtained with the records contained in their files.

The feasibility of implementing such a process will depend on the size of the network. Once you exceed 100 providers, however, manual processes become less feasible. At a certain point it is necessary to utilize technology to automate this process whereby Web-based databases are queried continuously to retrieve and update provider information. Such processes can cut the expense of continuous monitoring by 80 percent or more.

Verify the Important Data and Information

Ideally, each facility should verify the following credentials for all independent licensed practitioners in consideration of reviewing their initial application for clinical privileges or reapplication:

- state medical license;
- Drug Enforcement Administration (DEA) certificate and, if applicable, state equivalent;
- certificate of malpractice insurance;
- criminal background check and abuse registry check;
- professional references;
- questionnaire about disciplinary action, privilege restrictions, criminal violations, controlled substance violations, malpractice claims;
- query to the National Practitioner Data Bank;
- liability claims history;
- Office of Inspector General (OIG)/General Services Administration (GSA)/Office of Personnel Management (OPM) Excluded Parties List System (EPLS);
- government-issued picture identification;
- medical school residency/internships;
- fellowships/other professional training;
- Educational Commission for Foreign Medical Graduates (ECFMG);
- board certification;
- hospital affiliations; and
- work history review.

With the advent of sophisticated technology solutions, many facilities now are opting to outsource this functionality. Through a shared access platform, facilities can check status, generate reports, and even create Web-based privilege forms, schedule practitioners, and other features. Essentially, an organization can create a virtual medical staff office where all the systems are in one convenient electronic location, lower their costs of credentialing, and decrease their risk.

For facility staff, this solution also relieves burdensome repetitive tasks so that they can focus on the business of maintaining patient safety and providing services to their practitioners. Ongoing verification also means that there are no unwelcome surprises at the end of each day since facilities always know the status of credentialing activity. Outsourcing is becoming popular since it substantially eliminates credentialing paperwork, saves on data entry, eliminates costly subscriptions to reference sources, and ensures that the facility is compliant with regulatory requirements.

An increasing number of health care organizations are embracing this change and implementing new monitoring technologies to minimize risk to their patients and ensure against legal fall-out, making Web-based credentialing one of the latest and most promising tools for planning and implementing a compliance program that meets federal standards.

Endnotes:

1. Van Amerongen, Derek; *Physician Credentialing In A Consumer-Centric World*; Health Affairs; The Policy Journal of the Health Sphere; content.healthaffairs.org/cgi/content/full/21/5/152.

D. Scott Jones / Rory S. Jaffe

Patient Safety Organizations: Champions for Quality

D. Scott Jones, CHC, LHRM, is vice president of corporate compliance and risk management for American Healthcare Providers Insurance Services, a national professional liability insurance management company with headquarters in Philadelphia, PA. He has conducted quality and compliance assessments in over 1,000 health care organizations across the United States over the last decade. He can be reached at sjones@ahpis.com or by phone at 904/294-5633.

Rory S. Jaffe, MD, MBA, is executive director of CHPSO, the California Hospital Patient Safety Organization. He has extensive experience in both clinical care and health system leadership. He previously served as executive director of medical services for the University of California system. He is also past president of the Health Care Compliance Association (HCCA).

Hospitals, Providers, Clinicians, and Compliance Officers Have a New Means of Improving Quality and Compliance

The Patient Safety and Quality Improvement Act of 2005 (PSQIA, PL 109-41, 42 U.S.C. 299 b-21-b-29) included development of patient safety organizations (PSOs) as a means of allowing health care organizations, physicians, clinicians, quality, and compliance managers to share quality and incident data to improve the quality of care provided to patients.[1] The goals of PSOs include reducing the frequency of incidents that result in adverse patient outcomes and improving patient safety and the quality of care.[2] On November 21, 2008, 42 CFR Part 3, the Patient Safety and Quality Improvement: Final Rule appeared in the *Federal Register*, authorizing the creation of PSOs and invoking unique protections for the information shared with PSOs.[3]

In this article, we interview physician, compliance officer, and quality leader Rory Jaffe, MD, MBA, to learn more about PSOs and how they work to improve quality and compliance. Dr. Jaffe is the executive director of the California Hospital Patient Safety Organization (CHPSO), the second registered PSO established in the United States. He has a distinguished career as a physician, quality, and compliance officer and is the immediate past president of the Health Care Compliance Association (HCCA). He also established the first-ever national Compliance and Quality Conference that is now in its third year.

Promoting a Safety Culture; Protecting Incident and Patient Safety Data: Keys to Improving Quality

In the PSQIA, federal legislation recognized the need for health care providers, clinicians, hospitals, and health care organizations of all types to share data on incidents and quality improvement without fear of disclosure. The Patient Safety Act includes formidable protections against discovery, subpoena, and disclosure of information shared with PSOs for the purposes of improving patient safety.[4]

Are PSOs important to compliance officers? According to Dr. Jaffe, "Compliance officers have to be aware of PSOs and understand the privilege protections provided information shared with the PSO. The strong federal protections established in PSQIA apply to patient safety work product (PSWP). Specifically, PSWP is defined as "…any data, reports, records, memoranda, analyses (such as root cause analyses), or written or oral statements which are assembled or developed by a provider for reporting to a patient safety organization and are reported to a patient safety organization; or are developed by a patient safety organization for the conduct of patient safety activities; and which could result in improved patient safety, health care quality, or health care outcomes; or which identify or constitute the deliberations or analysis of, or identify the fact of reporting pursuant to, a patient safety evaluation system."[5]

PSQIA goes on to specify, however, that medical records, billing and discharge information, or other original patient records are not considered PSWP.[6] Also, from a systems standpoint, ultimately the culture of safety and the culture of compliance are very similar. Measuring these cultures requires asking the workforce many of the same questions, such as: Are you aware of problems? Are you comfortable discussing them without fear of reprisal? Is appropriate action taken when problems are identified?"[7] Compliance officers should collaborate with those working on patient safety to develop an organization with these four cultures of safety and compliance:

- Just culture: Errors and unsafe/improper acts will not be punished if the error was unintentional; however, those who act recklessly or take deliberate and unjustifiable risks will still be subject to disciplinary action.
- Reporting culture: People have confidence to report safety/compliance concerns without fear of blame. Confidentiality will be maintained, and the information they submit will be acted upon.
- Informed culture: The organization collects and analyzes relevant data and actively disseminates safety/compliance information.
- Learning culture: The organization is able to learn from its mistakes and make changes.

Patient Safety Work Product Protections

Protection of PSWP is a foundation of the effectiveness of PSOs. Organizations should carefully review the Act, the final rule, and consult with their PSO of choice (as well as competent legal counsel, if necessary) to consider protections and establish proper reporting systems. In addition to reading provisions of the Act, readers are directed to the final rule, specifically the section "When is information protected" at www.pso.ahrq.gov/regulations/2008-27475_pi-1.pdf (Accessed 5/14/09) for a detailed discussion of what information is, and what information may not be, protected.

Once PSWP enters the PSO system, it is protected from disclosure by layers of regulations, including Health Insurance Portability and Accountability Act (HIPAA), PSQIA, and civil monetary penalty protections. These protections are noted to extend broadly to:

> …patient, provider, and reporter identifying information….that is collected, created, or used for patient safety activities and imposes civil monetary penalties (CMPs) for impermissible disclosures of this information…[8]

CHPSO addresses the issues of discoverability of information and liability for that information at www.chpso.org:

> Until passage of the Patient Safety and Quality Improvement Act of 2005 (PSQIA), we did not have the appropriate tools to address systems issues and disseminate information learned from safety events. Quality improvement activities tended to be regulated by state laws, which generally addressed peer review of the qualifications and skills of individual practitioners. Systems review, and the types of activities that benefit systems learning, were not protected by the state laws. The lack of protection inhibited reporting and learning from these failures.
>
> Systems failures, unlike individual failures, are often best addressed by sharing the experience with others (e.g., other hospitals). The PSQIA recognizes this, and created PSOs as a method of sharing and analyzing information within a sphere of confidentiality for both patient and provider, and privilege from discovery.[9]

"Compliance officers and legal counsel need to study the confidentiality and privilege rules that are part of PSQIA," says Dr. Jaffe. "It is important to ensure the right kind of data is protected as patient safety work product. It is important to know that releasing information containing provider identification under PSWP protections requires consent of all health care providers who are affected.

"The strong protection for PSWP means that for the first time we can talk about and share information across our health system without fear of discovery. We can talk about problems. We can write emails about concerns. We can hold meetings and openly discuss issues and needs, and all of these actions are protected as long as the PSWP privilege is properly invoked," he adds.

PSOs also allow health care providers and organizations to aggregate data from a large number of sources to better analyze issues that may affect patient safety. Prior to the Patient Safety Act, safety concerns seldom were analyzed across a variety of health care providers and institutions, due in large part to fears of discovery. The PSO will be able to produce detailed analysis of patient injury events and incidents, depending on the quality and quantity of data collected by health care organizations that become its members.[10]

The significance of this ability to share data is immediately clear: Health care facilities and providers will now be able, through PSOs, to develop and obtain national benchmarks for safety and quality improvement. Aggregated data also will allow an understanding of the systems issues behind the event — a perspective that frequently requires comparison of experiences among many providers.

They can use these comparisons to evaluate their own experiences and improve processes. Instead of working to improve safety in isolation, health care providers can share information that can provide means for a unified approach to improvements. Forward-thinking organizations can use data from the risk experiences of other organizations to design new approaches and identify concerns that have not yet resulted in injuries in their own facilities.

Establishment of these unique federal protections gives health care organizations and providers a unique new ability to share data, develop information on patient safety and injury events, and develop solutions to common problems. The potential impact on improving quality of care and reducing patient injuries is huge. The PSO is a huge leap forward in the ability of health care organizations to improve quality. To serve effectively, PSOs now need patient safety data from health care providers.

Setting up Internal Systems for PSWP

A large part of preparing to effectively utilize membership in a PSO involves setting up internal policy and procedure that will organize a patient safety evaluation system

(PSES). The PSES is a process of including information in a protected investigation process and establishing patient safety work product protections.

"The workflow process may include instruments that collect incident or event data, communications between investigating staff, memos, medical staff reports, even email messages between involved staff members," says Dr. Jaffe. "It is important to fully understand the internal PSES described in detail in PSQIA and the final rule."

He also notes that once information enters the PSES, it may be extracted from the system only before submission to the PSO. "Let's say a medical staff recognizes that a series of patient injury events reveals a need to report a provider. Information can be extracted from the PSES and used to make a report to the Board of Medical Examiners, for example. And, of course, mandatory state reports must still be made, even though data may also be in the PSES. If the information in the PSES has already been reported to a PSO, the provider may have to independently recreate the report. Therefore, timing of PSO submission and coordination with reporting requirements is important."

Choosing a PSO

CHPSO was the second PSO in the country registered with the Department of Health and Human Services (HHS) and the Agency for Healthcare Quality and Research (AHRQ). It is one of only 59 PSOs listed by AHRQ as of the time this article was written. Only PSOs listed with HHS and AHRQ and displayed on the AHRQ Web site are qualified to receive and use provider information on patient safety events or incidents.[11] A list of the 59 approved PSOs (as of the time of this article) can be seen on the HHS/AHRQ PSO Internet site at www.pso.ahrq.gov/listing/psolist.htm (Accessed 5/12/09).

"PSOs are governed by a bazillion regulations," says Dr. Jaffe. A review of the PSO application for listing with HHS reveals a small part of the difficulty involved in establishing a PSO. The application form requires extensive and detailed information.[12] In addition, PSOs must follow a specific scope of required work. The patient safety activities required under 42 USC include:

- efforts to improve patient safety and the quality of health care delivery;
- the collection and analysis of patient safety work product;
- the development and dissemination of information with respect to improving patient safety, such as recommendations, protocols, or information regarding best practices;
- the utilization of patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk;
- the maintenance of procedures to preserve confidentiality with respect to patient safety work product;
- the provision of appropriate security measures with respect to patient safety work product;
- the utilization of qualified staff; and
- activities related to the operation of a patient safety evaluation system and to the provision of feedback to participants in a patient safety evaluation system.[13]

Understanding the extent of regulations governing PSOs can alert health care providers and compliance officers that PSOs are a protected and structured environment for sharing patient safety data and using that data to improve outcomes. Federal support for PSOs is strong from regulatory agencies and even lawmakers. "PSQIA passed with a unanimous Senate vote and had only three no-votes in the House," notes Dr. Jaffe.

So how do you choose the right PSO? Dr. Jaffe notes that there are no prohibitions against joining multiple PSOs that serve different needs. He notes that most organizations will choose a primary PSO — typically one that focuses on a type of provider (*e.g.*, hospitals). They also may select a geographically localized organization that will allow all providers in an area to share experiences and information across the entire continuum of care. "It makes sense for organizations to join a PSO operating in their geographic area," he says. "Providers need to be able to talk to one another." He notes that PSOs may be provider or medical service specific and may be centered in unique areas like metropolitan centers or rural settings.

CHPSO is an example of a hospital-focused regional model. CHPSO is focused on California hospitals and improving outcomes in that state. Like many other statewide PSOs, it will focus on patient safety initiatives, laws, and regulations that are specific to its geographic region. A benefit of this approach is that it may allow a PSO to share information with a group of hospitals in a way that allows all facilities and health care providers in that network to address safety concerns and improve simultaneously.

PSOs also can work collaboratively across state lines, however. For example, on February 19, 2009, CHPSO was selected as one of the state hospital associations and PSOs to participate in a demonstration project that will study how to reduce central catheter line associated bloodstream infections in hospital intensive care units (ICUs). According to the press release from AHRQ, hospital associations in 10 states were selected to participate in the project. "States are California, Colorado, Florida, Massachusetts, Nebraska, North Carolina, Ohio, Pennsylvania, Texas, and Washington. In addition, the California Hospital Patient Safety Organization, the North Carolina Center for Hospital Quality and Patient Safety, and the Ohio Patient Safety Institute will participate in the project…"[14]

Ultimately, AHRQ plans to aggregate deidentified data from many PSOs into a national patient safety database. The deidentification will be performed by the PSO Privacy Protection Center.

PSO Cost

"The PSO will be a small organization in most cases," says Dr. Jaffe. "Cost of joining should not be excessive." PSOs also provide a significant economy of scale: not only leveraging the PSO employees' skills among many providers but also allowing the providers themselves to share talents and insights of each others' workforce.

A review of a variety of PSO Internet sites reveals that many offer packages of services, all of which are voluntary. Some offer very specific services, such as the ability to provide information or intervention in a specific patient safety event or incident. These enhanced services may include root cause analysis, continuing medical education (CME) related to improving specific instances of performance, or other programs. The cost of joining a PSO should be well outweighed by the benefits of being able to share information with peers in a protected manner and develop better patient safety systems.

PSOs and the Future of Health Care

"Health care has become more effective but at the same time has become more complex and dangerous. The establishment of PSOs is all about redesigning health care delivery systems," Dr. Jaffe concluded during our interview for this article. "PSOs should help us figure out how to deal with human fallibility…including issues like workload and information overload. The practice of medicine must change. To be safer we need to redesign our delivery systems to accommodate human fallibility. This will require a number of new practices, such as establishing reproducible procedures in medicine — like the extensive checklists that helped make the aviation industry one of the safest means of travel in the world."

Endnotes:

1. The Patient Safety Act, PL 109-41, 42 U.S.C. 299 b-21-b-29 is available in its entirety at www.pso.ahrq.gov/statute/pl109-41.htm (Accessed 5/6/09).
2. U.S. Department of Health and Human Services (HHS), Agency for Healthcare Research and Quality (AHRQ), Patient Safety Organization Information, www.pso.ahrq.gov/psos/overview.htm (Accessed 5/6/09).
3. Federal Register / Vol. 73, No. 226 / Friday, November 21, 2008 / Rules and Regulations, p. 70732, www.pso.ahrq.gov/regulations/2008-27475_pi-1.pdf (Accessed 5/6/09).

4. U.S. Department of Health and Human Services (HHS), Agency for Healthcare Research and Quality (AHRQ), Legislation and Regulations www.pso.ahrq.gov/regulations/regulations.htm (Accessed 5/6/09).
5. The Patient Safety and Quality Improvement Act, PL 104-41, 42 U.S.C. 299b-21, (2)-(7), Definitions, Pp. 118-119, www.pso.ahrq.gov/statute/pl109-41.htm (Accessed 5/14/09).
6. Ibid.
7. Interview with Rory Jaffe, MD, MBA, executive director, the California Hospital Patient Safety Organization (CHPSO), May 13, 2009. CHPSO was the second PSO registered with HHS and AHRQ in the United States. To learn more about CHPSO and PSOs, visit www.chpso.org.
8. U.S. Department of Health and Human Services (HHS), Office for Civil Rights, Delegation of Authority, www.hhs.gov/ocr/privacy/psa/understanding/delegationofauthority.html (Accessed 5/6/09).
9. California Hospital Patient Safety Organization (CHPSO), "What is CHPSO?" www.chpso.org (Accessed 5/6/09).
10. U.S. Department of Health and Human Services (HHS), Agency for Healthcare Research and Quality (AHRQ), Patient Safety Organization Information, www.pso.ahrq.gov/psos/overview.htm (Accessed 5/6/09).
11. U.S. Department of Health and Human Services (HHS), Agency for Healthcare Research and Quality (AHRQ), Alphabetical Directory of Listed Patient Safety Organizations, www.pso.ahrq.gov/listing/alphalist.htm (Accessed 5/6/09).
12. Department of Health and Human Services (HHS), Agency for Healthcare Quality (AHRQ), PSO Registration Form, www.pso.ahrq.gov/listing/certfm.pdf (Accessed 5/12/09).
13. The Patient Safety and Quality Improvement Act, PL 104-41, 42 U.S.C. 299b-21, Patient Safety Activities, www.pso.ahrq.gov/statute/pl109-41.htm (Accessed 5/12/09).
14. U.S. Department of Human Services (HHS), Agency for Healthcare Research and Quality (AHRQ), Press Release, "10 State Project to Study Methods to Reduce Central Line-Associated Bloodstream Infections in Hospital ICU's" www.ahrq.gov/news/press/pr2009/clabsipr.htm (Accessed 5/6/09).

Richard P. Kusserow

Disclose or Not Disclose: That Is the Question

When Deciding Whether or Not to Self Disclose, Carefully Review OIG Guidance on the Subject

Richard P. Kusserow is the former HHS Inspector General and is chief executive officer of Strategic Management Systems, Inc., which has been providing specialized compliance advisory services since 1992. For more information, see www.strategicm.com or call him directly at 703/535-1411.

Our firm has been engaged in reviewing claims and arrangements for a great many hospitals. Invariably, we find errors, omissions, and other irregularities. Always the question is raised with trepidation as to whether the findings should result in disclosure to the Department of Health and Human Services (HHS) Office of Inspector General (OIG). In only a handful of cases has the answer been in the affirmative.

It is clear from our experience that many do not fully understand the guidance offered by the OIG on the subject and have been self disclosing when it was not necessary. The purpose of this article is to help provide better understanding of when disclosure should or should not be made to the OIG.

For a number of years, the OIG has sought to encourage health care provider voluntary disclosure of improper conduct. It has done this through a variety of written guidance designed to clarify when self referrals are appropriate and when they are not. The primary guidance document on this was through the self-disclosure protocol (SDP) issued by the OIG in 1998. It stated:[1]

> The OIG has long stressed the role of the health care industry in combating health care fraud and believes that health care providers can play a cooperative role in identifying and voluntarily disclosing program abuses. The OIG's use of voluntary self-disclosure programs, for example, is premised on a belief that health care providers must be willing to police themselves, correct underlying problems and work with the Government to resolve these matters.

Since it was first published, the SDP has been used by a significant number of providers who discover compliance problems and want to correct the problems, repay any overpayment, and move forward with a clean slate. This process can provide the provider with an effective and relatively efficient means of resolving liabilities and avoiding becoming a defendant in a future False Claims Act (FCA) case. The OIG has stressed that voluntary self disclosure would result in a payment that would be less than those in which the government found the problem independent of the entity. It has remained faithful to that promise in that payments have been at a far lower rate for those parties engaged in the SDP as opposed to the alternative.

Disclosures have fallen into two broad categories — those involving overpayments arising from violations of law or regulations and improper arrangements with referral sources.

The OIG suggested that the SDP is to be used after a provider conducts an internal review indicating that a problem exists that may implicate violations of federal criminal, civil, or administrative laws. In the last 10 years, the OIG has accepted upward of 500 disclosures; about half of the disclosures for overpayments were not resolved through the SDP process but rather referred to the Medicare contractors for resolution.

When making a decision as to whether to self disclose overpayments, it is advisable to look to the OIG guidance on the subject. The OIG stated that its SDP is not to be used to report routine overpayments or errors:[2]

> Matters exclusively involving overpayments or errors that do not suggest violations of law have occurred should be brought directly to the attention of the entity (e.g., a contractor such as a carrier or an intermediary) that processes claims and issues payment on behalf of the Government agency responsible for the particular Federal health care program (e.g., [CNS] for matters involving Medicare). The program contractors are responsible for processing the refund and will review the circumstances surrounding the initial overpayment.

The second general category in which the OIG has accepted and resolved matters brought to its attention under SDP involved matters involving potential violations of the anti-kickback statute and the Stark laws. This category is likely to be much more serious, especially when involving the anti-kickback statute, a criminal statute. It is also an area in which the OIG and the Department of Justice (DOJ) receive predicating case information through the *qui tam* provision of the FCA (the so called "Whistleblower Act"). Complicating matters is that a self disclosure does not necessarily bar a relator or even DOJ from pursuing an FCA action.

Anyone reviewing the DOJ settlement agreements in health care or the OIG corporate integrity agreements (CIAs) and certificate of compliance agreements (CCAs) will notice that the great majority of them are under the FCA but predicated by the violations of the anti-kickback statute. Often, Stark law violations are coupled with the anti-kickback statute in a case.

When a provider discovers compliance problems involving the Stark law alone, the protocol has not worked as well as other forms of SDP. The fact is that so many providers have self disclosed Stark violations that the OIG felt the need to clarify the SDP in that context.

On March 24, 2009, the OIG issued an open letter to health care providers providing further clarification regarding the use of its SDP. Due to resource constraints, the OIG advised that its SDP will no longer be available to solely report violations of the Stark law. It will only accept future self disclosures under the Stark law if they

Continued on page 67

Betsy McCubrey / John Rah

Pharmaceutical Manufacturer Payments to Physicians — It's Time for You to Show Your Hand

Betsy McCubrey and **John Rah** are partners at the law firm of Morgan Lewis & Bockius. Both attorneys are members of the international health law practice and represent pharmaceutical companies on compliance and related issues.

The Trend toward Greater Transparency of Physician Relationships Is Not Losing Steam

The April 28, 2009, Institute of Medicine's (IOM's) *Conflict of Interest in Medical Research, Education, and Practice* report offered the latest in the movement toward greater physician relationship transparency in the pharmaceutical industry. This movement is reflected in various state law reporting requirements, recent corporate integrity agreements (CIAs) executed with the Office of Inspector General (OIG) and deferred prosecution agreements with the Department of Justice (DOJ), voluntary efforts by pharmaceutical and device manufacturers themselves, and proposed federal legislation such as the Physician Payments Sunshine Act.

While it appears clear that the movement toward greater transparency is going to continue forward, what remains to be seen is what form it ultimately will take and what consequence there is for those subject to the new requirements. We discuss in this article some of the recent significant requirements and developments involving physician relationship transparency.

Corporate Integrity Agreements

The recent CIAs entered into by Cephalon, Inc. and Eli Lilly and Company[1] with the OIG of the Department of Health and Human Services (HHS), like the September 2007 device industry settlements, require both Cephalon and Eli Lilly to disclose, via their Web sites, all direct and indirect payments to physicians.[2] These CIAs define the term "payments" as payments or transfers of value, whether in cash or kind, including payments or compensation for services rendered, grants, fees, honoraria, payments for research or education, food, entertainment, gifts, trips or travel, products or items provided for less than fair market value, or other economic benefit.[3]

The CIAs require reporting aggregate amounts, from $0 to $10,000, $10,001 to $20,000, et cetera per physician for the proceeding quarter. Included among the information that must be reported is the amount, in the manner listed above, the physician's full name, and the city and state of the physician's practice.[4] The language of the CIAs does not distinguish between payments associated with consulting arrangements and other arrangements, including clinical research arrangements and surveys.

Given the OIG's historic trend to include existing CIA requirements in new agreements into which it enters, there is little reason to believe that pharmaceutical and device manufacturers entering into future CIAs will not be subject to the same or similar requirements.

The Physician Payments Sunshine Act

While the OIG has been working to enhance transparency through its CIAs, Congress has been working on its own initiatives to bring greater transparency. On January 22, 2009, Senate Finance Committee Ranking Member Chuck Grassley (R-Iowa) introduced S. 301, the Physician Payments Sunshine Act of 2009. The yet unpassed Act proposes an amendment to Title XI of the Social Security Act by adding a new section entitled, "Transparency Reports and Reporting of Physician Ownership or Investment Interests."

Of particular note is the bill's requirement of disclosure of payments made to physicians, physician medical practices, or physician group practices by drug and device manufacturers. Payments (or other transfers of value) include (1) gifts, (2) honoraria, (3) speaking fees, (4) consulting fees, (5) travel, (6) services other than consulting, (7) entertainment and food, (8) education, (9) research, (10) charitable contributions, (11) royalty or license payments, (12) grants, (13) dividends, (14) profit distributions, (15) stock or stock option grants, and (16) ownership or investment interests.

While there are several exceptions, including aggregate payments of less than $100 during the calendar year, discounts (rebates), and certain educational items, such exceptions are limited. The Act specifies that the initial report would come in the form of an annual report to Congress with more limited summaries to the states.

Thereafter, in 2011, the reports would need to be available to the public (by the manufacturer) via Internet Web site and would need to include the name and business address of the physician, the date of the payments, the value of the payments, and a description of the form and nature of the payment. Additionally, the name of the covered drug also would need to be disclosed in certain circumstances. Notably, unlike a previously proposed version of a similar bill, the Act is applicable to all manufacturers of covered drugs as well as devices, biologicals, and medical supplies.[5]

Voluntary Disclosures by Pharmaceutical Manufacturers

Some pharmaceutical manufacturers have taken the initiative on transparency efforts and have committed to release certain information about their own payments to physicians. For example, in February 2009, Pfizer Inc., the world's largest drug manufacturer, announced its plans to make publicly available its compensation of U.S. health care professionals for consulting, speaking engagements, and clinical trials. The disclosure will include payments made to practicing U.S. physicians and other health care providers, as well as principal investigators, major academic institutions, and research sites for clinical research.

This voluntary disclosure will make Pfizer the first biopharmaceutical company to commit to reporting payments for conducting Phase I-IV clinical trials in addition to disclosing payments for speaking and consulting.[6] The payments include those for:

- clinical development and commercial consulting;

Continued on page 68

Cindy Schroeder

Is It Necessary to Write a Policy on How to Write a Policy or Template?

Cindy Schroeder, LPN, BS, CPC, CPC-H, is employed at MeritCare Health System, a not-for-profit integrated health care system headquartered in Fargo, ND. Her primary function is policy coordinator and internal auditing for compliance.

What's Next…Directions on How to Follow Directions?

Due to the enormity of this subject, this article will be split into two parts. Part I will focus on creating the baseline for writing a policy and creating the foundation for how a policy should be written. Part II will focus on implementation and the processes in developing and maintaining a fluent policy structure.

I recently had an opportunity for a career change that led me to coordinate a massive (and quite disorganized) online policy system throughout our current health system. Our health system is one of the largest hospital/clinic systems in the upper northwest. Our services range from critical access and trauma center to numerous regional clinics in multistates all encompassing over 73 specialties.

After the first few days of my new career, I started reviewing the abundant online policies and realized how dysfunctional many were. There were duplicates in various departments and mixed information; some were not even policies but forms and checklists. How did we get to this level? Where do I begin?

Realizing the enormity of what I had gotten myself into, I could not help but drift back to a much simpler time in my life — a time where skipping rocks and playing hopscotch engulfed my days. I had this urge to call my mommy, and she would make it all better with a kiss and a band-aide. It then dawned on me: someone had to teach me how to skip on one foot to play hopscotch. Someone had to show me how to look for that flat rock and hold it just right so that it skipped across the water.

Have we gotten so technically advanced that we have forgotten the basic informational tools needed to function? I had to create and teach the foundation of simple basics. I had to create a "policy on policies."

Where Do I Begin?

If you already use or plan to use a templated online system policy format, coteam this first stage with an associate in your computer/technical department. With your tech team, you will need to create the format you want as well as what fields and headers are desired. You must set this up before you can create your policy on policies.

Your policy on policies and template format must be in the same criteria format that you expect others to adhere and available to policy writers. There are many other advantages that can be helpful down the road, such as data fields for reporting, which you will find in more detail in Part II of this article.

Once you have decided what fields you want mandated for all policies (*e.g.*, "Title" and "Purpose"), you can go ahead and start your policy on how to create a policy.

The Policy

Data Fields/Titles/Headers

As noted above, the policy should clarify what will be *mandated* fields verses *suggested* fields in your online template (*e.g.*, headers, format, and content).

Roles and Responsibilities

Outline the roles and responsibilities of the policy coordinators, editors, managers, and others who create and maintain policies. Enforce the fact that all employees are responsible for familiarizing themselves with your facility policies — not only where they are located but any policy that is pertinent to their current practice and environment.

Standardization and Approval Process

Outline the process for policy implementation and processes for new, revised, and retired or archived policies. This information is dependent on how you structure your format and processes dependent on the needs and tools with which to work.

Policy Development

Research

The department with the most ownership of a subject matter should be accountable for creation and all research relating to that policy. Reason being, the policy may affect greatly one or more other department areas. Make sure the policy on policies clarifies that the policy writer collaborates with other departments that have a vested role and interest in the subject matter. This is to avoid duplication and mixed information of policies regarding the same subject throughout your system.

Standardization

The title of your policy *must be pertinent to the subject matter*. The first word of the title is critical, and you should avoid using terms such as policy, policy for, manual, or the name of your company. For example, do not have a policy titled "Smith Cleaning Service Policy for Time Off." If you had Smith Cleaning Service in every title and someone wanted to do a search on "cleaning with disinfectants," it would take quite a bit of time to sort through and find the policy you are looking for because every policy would come up with the word "cleaning" (since it is in the title of the company).

The policy must be *clearly written* and in a concise manner. It should be in a step-by-step framework that can be understood easily by someone not working in that area. Is there a piece of equipment or a procedure that other associates would not be familiar? Use common, everyday words, and avoid abbreviations and symbols. For example, could you understand and follow a policy from construction or accounting? If you have to use specific words not commonly understood by others, add a list of definitions in the policy.

The policy should use gender neutral language and job titles instead of personal names. For example, the policy should say "The manager of surgical services" instead of "Mary Smith in surgery."

Continued on page 69

RITA A. SCICHILONE

Are We There Yet? Compliance-Ready Computer-Assisted Coding

Rita A. Scichilone, MHSA, RHIA, CCS, CCS-P, CHC, is a director of Practice Leadership for the American Health Information Management Association. She may be contacted by email at Rita.Scichilone@ahima.org.

New Technologies Help Organizations Work Smarter Toward Compliance-Ready Systems

Nine years ago a report was issued by the Department of Health and Human Services Office of Inspector General (OIG) entitled "Medical Billing Software and Processes Used to Prepare Claims."[1] This report stated that "diagnostic and service information about a patient visit is rarely coded directly into medical billing software by physicians and other medical service providers." Coding is a complex activity requiring knowledge of the coding systems used, the source document subject matter, and any guidelines or rules required for external reporting or internal use of the data.

Those little numbers or alpha-numeric strings are one of the reasons the compliance profession exists. The codes communicate both the "what" (services rendered, supplies used, substances administered) and the "why" (medical necessity, reason for visit, diagnostic information) on claim forms for external use and facilitate indexing and information retrieval for internal purposes.

Electronic health records and innovation in technology and communication has changed significantly since the OIG report warned about risk of software programs "intentionally designed to produce improper or inaccurate claims." Market research shows that there are considerably more options in the marketplace related to what an American Health Information Management Association (AHIMA) work group defined as computer-assisted coding in 2004.[2,3]

WHAT IS COMPUTER-ASSISTED CODING?

Computer-assisted coding is the use of computer software that automatically generates a set of medical codes for review and validation or use based upon clinical documentation provided by health care practitioners.[4] The current Health Insurance Portability and Accountability Act

(HIPAA) code sets ICD-9-CM and HCPCS/CPT® for the ASC X12N Professional and Institutional Health Care Claims require human oversight to ensure correct classification and adherence to coding guidelines for most code assignment. Diagnostic coding in particular requires record analysis and application of coding conventions and guidelines.

There are examples of fully automated coding routinely used in health care operations without significant data integrity issues. When a service can be linked to a corresponding code without loss of meaning, it is wasteful to require a person to assign codes when a computer can do it faster and cheaper. Just as an account number is used to retrieve financial data (*e.g.*, bank account, credit card transaction, et cetera), "chargemaster or charge description master" software links services with corresponding codes for billing and claims submission.

When well designed and maintained, software solutions facilitate data integrity checking and save money. The current coding workflow is resource intensive because it requires manual analysis of the source document for codeable conditions and services, retrieval of the appropriate codes, application of guidelines, then reentry of the coded data into systems for other uses.

Computer-assisted coding software provides recognized advantages, including:

- increased productivity in code assignment;
- enhanced coding made possible by built-in compliance prompts and reminders and "on board" clinical references;
- consistent application of reporting rules and guidelines; and
- electronic audit trails and enhanced monitoring and evaluation features for coding accuracy reviews.

Compliance concerns by health care providers have been voiced as one of the barriers toward automation of code assignments. Health record documentation is a complex process with wide variation between location and type of facility. The potential for errors in code assignment affecting reimbursement is a significant concern, both to facilities and payers. The added costs, along with a lack of industry standards or certification of CAC system software functionality, are factors affecting widespread adoption. Measurable standards are required to confirm that CAC software systems are reliable enough to satisfy data integrity needs for providers, payers, and patients.

The requirement to adopt ICD-10-CM and ICD-10-PCS by 2013 has prompted additional inquiries about automated solutions from the health care community. The sheer number of diagnostic codes, procedure codes, and coding requirements were stated to be a factor for billing errors in the OIG report.

ICD-10-CM has more than five times as many codes as ICD-19-CM (68,000 compared to 13,000) with the procedure coding system (ICD-10-PCS) exponentially larger by design. In a classification system, the larger number of available codes facilitates linkage between health record entries and the codes since both systems provide usability improvements over the 30-year-old ICD-9-CM.

Electronic health records (EHRs) also are expected to be an enabling factor. Well-designed EHR systems will allow physicians to enter codified information at the point of care into template fields with the assistance of user-friendly interfaces. Just like account numbers facilitate data integrity and information retrieval, codes have a role to play in improving the utility and accuracy of health records for all stakeholders, including the patient.

Improperly designed input methods include:

1. limitation of coding options to providers such as a template or pull down menu that restricts choices to "covered or payable" service codes;
2. fragmented procedure codes resulting in unbundling of charges;
3. replication functionality that enables copy of record entries from one record to another without detection;
4. steering users of the software to higher valued procedure codes than the service documentation supports;

Continued on page 69

Melinda S. Stegman

End-Stage Renal Disease Facility Composite Rate: What's Separately Billable and What's Not?

A Large Proportion of Claims Could Be Billed Inappropriately If Facilities Fail to Pay Close Attention

Melinda S. Stegman, MBA, CCS, is a clinical technical editor at Ingenix.

Ensuring compliance with billing guidelines related to bundled services is one of the more difficult issues to control in the hospital-based and independent dialysis facility settings. As a result, there may be a significant proportion of claims inappropriately billed with separate codes for laboratory services.

The Office of Inspector General (OIG) released a report in April 2009 — the findings of which included an estimate of $3.9 million in overpayment for these services during calendar years 2004–2006. A small portion of this amount involved separately billable tests that were billed beyond the allowed frequency without required medical documentation and a small number of claims with undocumented test charges (*i.e.*, no evidence that the tests were performed).

The Centers for Medicare & Medicaid Services (CMS) has established a composite payment rate for both hospital-based and independent dialysis facilities, which is considered a comprehensive payment for all services related to dialysis treatment, with the exception of physician professional services and certain drug and laboratory services that are separately billable. In addition, CMS specifies the frequency (*e.g.*, per treatment, daily, weekly, or monthly) with which the tests are reimbursable. In some cases, the tests may be performed at a higher frequency and may be reimbursable if they are medically justified by medical documentation.

Scope of Review

The OIG's review covered 339,342 claims totaling $7,381,070 provided by 326 dialysis facilities in calendar years 2004–2006. National Government Services (NGS) was considered the fiscal intermediary for the claims reviewed for this project. The review was conducted between October 2007 through May 2008 and involved 125 dialysis facilities in the sample.

Using CMS' national claims history file, end-stage renal disease (ESRD) composite rate paid claims were matched with the dialysis facilities' ESRD outpatient laboratory claims based on "from" and "through" dates. The concept of "beneficiary quarters" were used, which is comprised of all separately billed and reimbursed services that are subject to ESRD payment requirements that were performed for an ESRD beneficiary during a calendar quarter.

Billing records, medical records (including dialysis treatment dates, physician orders, laboratory tests performed, and progress notes), claims, and remittance advice information was reviewed and compared. Generally accepted government auditing standards were followed, and all applicable Medicare laws, regulations, and guidance were applied. There were 12 different NGS contracts for ESRD services during this time period; a stratified random sampling methodology made up of 12 strata was used, one for each of the 12 NGS contracts.

General Findings

It was determined that many of the facilities had billed inappropriately for the laboratory tests because they did not have sufficient controls to ensure that all claims complied with Medicare requirements. In addition, NGS had limited ability to identify the billing errors in its claim-processing system. The findings included the following:

- ESRD-related laboratory tests were appropriately billed and paid in 90 of the 360 beneficiary quarters that were sampled.
- In the remaining 270 beneficiary quarters, the facilities were inappropriately paid a total of $11,325 for the following reasons:
    - 347 beneficiary quarters contained errors totaling $10,273 for laboratory tests included in the composite rate that should not have been billed separately;
    - 32 beneficiary quarters contained errors totaling $827 for separately billable lab tests that were billed beyond the allowable frequency but without required additional medical documentation; and
    - nine beneficiary quarters contained errors totaling $225 for undocumented lab tests (*i.e.*, no evidence could be produced to substantiate that the tests were performed).

There are more than 270 beneficiary quarters in the individual error categories because some beneficiary quarters had more than one type of error.

Discussion

So how can ESRD providers ensure that the claims are appropriate and only reimbursable services are reported? First, it is important to understand what is included in the composite rate and what is separately billable. Secondly, regulations related to frequency should be reviewed carefully and disseminated to all staff responsible for coding or billing for ESRD patients.

CMS uses the 50 percent rule to determine reimbursement for automated multichannel chemistry (AMCC) tests, which specifies whether CMS will pay for the laboratory services separately. Specifically, the Medicare Claims Processing Manual, Pub. No. 100-04, Chapter 16, Section 40.6.1, states:

- "If 50% or more of the covered tests [on a given date of service] are included in the composite rate payment, then all submitted tests for that date are included in the composite rate payment. In this case, no separate payment in addition to the composite rate is made for any of the separately billable tests.
- If less than 50% of the covered tests on a given date of service are composite rate tests, all AMCC tests submitted for that date for that beneficiary are separately payable."

ESRD providers should be aware, however, that it is their responsibility to identify the AMCC tests ordered that are included in the composite rate and those that are not. The following are examples of inappropriately billed tests. Further, the manual, chapter 11, section 30.2.1.B indicates that:

> Certain separately billable lab tests (i.e., serum aluminum and serum ferritin) are covered routinely, i.e., without documentation of medical necessity other than knowledge of the patient's status as an ESRD beneficiary, when furnished at the specified frequencies. If they are performed at a frequency greater than once every three months, they are covered only if accompanied by medical documentation. A diagnosis of ESRD alone is not sufficient documentation. The medical necessity of the test(s), the nature of the illness or injury (diagnosis, complaint, or symptom) requiring the performance of the test(s) must be present on the claim. Such information must be furnished using the ICD-9-CM coding system.

Example 1: Tests Included in the Composite Rate

Patient #1 had blood drawn (*i.e.*, specimen collection) for a hemoglobin test with each dialysis treatment. Specimen collection and one hemoglobin test are included in the composite rate for each treatment. The dialysis facility, however, separately billed NGS for both the specimen collection services and the test each time the test was performed.

Example 2: Separately Billable Composite Rate Tests Billed Without Accompanying Documentation

Patient #2 had a potassium test four times during May in conjunction with her dialysis treatments. One potassium test is included in the composite rate each month. The dialysis facility separately billed NGS for three potassium tests performed in May after the first test. The medical records provided by the facility did not contain any documentation that medically justified the three additional tests.

Example 3: Payment Determinations Using the 50 Percent Rule; Incorrect Coding

Patient #3 had a calcium test and phosphorus test (both AMCC composite rate tests) on a single date of service. According to the dialysis facility's records, this date of service was the only time during the month that these two tests were performed. Therefore, the tests were composite rate tests within the specified frequency.

The facility, however, incorrectly coded the claim to indicate that the tests were composite rate tests beyond the specified frequency. NGS applied the 50 percent rule and thus separately paid for both tests. Because 100 percent of the tests actually performed were composite rate tests, these two tests were not separately payable.

Example 4: Payment Determinations Using the 50 Percent Rule; Incomplete Billing

Patient #4 had 10 AMCC tests on a single date of service. According to the facility's records, six of these tests were composite rate tests within the specified frequency, and four were not composite rate tests. The facility, however, billed only for the four noncomposite rate tests and did not include the six composite rate tests on the claim. Because of this omission, NGS calculated that 100 percent of the tests were not composite rate tests and separately paid the claim based on the 50 percent rule. Because 60 percent of the tests were actually composite rate tests, none of the 10 tests were separately payable.

Conclusions

The OIG recommended that NGS coordinate with CMS and other involved MACs to:

- conduct post-payment reviews of claims submitted by dialysis facilities that separately billed ESRD laboratory tests to

identify and recover overpayment estimates at $3.9 million, and
- educate dialysis facility staff about Medicare ESRD billing requirements related to the types of errors identified in the review.

Staff involved in any of the coding or billing activities for ESRD and dialysis facilities — whether hospital-based or standalone — should review billing requirements carefully. The OIG's full report may be viewed at the following link: oig.hhs.gov/oas/reports/region1/10700522.pdf. Appendix A details the laboratory tests subject to composite rate billing requirements, along with their corresponding current procedural terminology® (CPT®) codes and specific billing frequency limits.

CHRISTOPHER YOUNG

Electronic Health Records Pose Potential Compliance Liabilities for Clinical Laboratories

Now is the Time to Prepare by Understanding the Lab's Role and What Needs to Be Done

Clinical laboratories are unique in the Medicare regulatory and payment systems for many reasons. The rush to implement electronic health records (EHRs) and e-prescribing systems to grab some share of the government funding that may be associated with that, as well as to obtain the reimbursement gains provided through EHR demonstration adoption, has created a risk environment with implications for laboratories in the area of Stark and anti-kickback regulations that may not exist for other providers.

Part of the reason for this additional risk is that labs, unique among all other providers, have been providing legally, and relatively unchecked, free computers to their referral sources since the early 1990s. While use of these devices was limited to ordering tests and receiving results, they often incorporate medical necessity checking, the ability to review cumulative results on a patient, other test-related activities, and in many cases are interfaced with the physician office computer system to facilitate the entry of patient information into the lab's computer system.

It is only recently that hospitals, pharmacies, and other providers and suppliers have been permitted to provide hardware and software to physicians, albeit for a different purpose, but the presence of a lab computer in an office where a hospital or health system's EHR system is going to be installed can create problems. Also, there may be different issues when the laboratory is an independent lab as opposed to a hospital lab.

This column will overview briefly these risks, and even though it is still early in this effort, laboratories need to be aware of the potential issues because the investment in these systems can be substantial, there is

Christopher Young, CHC, is the president of Laboratory Management Support Services (LMSS) in Phoenix, Ariz. He can be reached at 602/277-5365 or by email at cpyoung@labcomply.com.

a focus by the government fraud detection agencies on Stark and anti-kickback regulations, and the consequences of violating Stark and anti-kickback regulations can be significant.

Barriers to Adoption of EHRs

The single largest deterrent to physician adoption of an EHR system is cost. Those who support the adoption of EHRs as a way to reduce costs in health care are looking at benefits to the entire health care system through improvements in quality of care and reduction of costly errors and duplication in the system with the benefit coming over a long period of time. Many of these benefits do not directly impact physicians in their office.

In fact, in the short term, there is a large upfront investment in hardware, software, maintenance, and retraining of employees with no guarantee of any near-term return on that investment. Further, changes in workflow while adopting these systems can affect their productivity and actually shift work that may have been done easier or mostly by an ancillary provider, like a laboratory, into the physician office with no direct benefit to the physician.

A second important consideration raised by physicians and hospitals, as well as others in the health care system, and closely related to cost, were certain regulations that prohibited larger providers like hospitals, insurers, and pharmacies from providing the hardware and software to physicians to help them with the cost. These larger entities gain the most benefit from a systemwide adoption of EHRs and would be willing to provide support for physician adoption by providing hardware and software but for the anti-kickback and Stark laws that prohibit them from doing so.

The Government's Solution

Recognizing the cost barrier, the government proposed incentives through changes in payment policy, for physicians and others who adopted EHR and e-prescribing systems. Demonstration projects were created to determine the most effective approach. The basic idea was that if you adopted some kind of EHR or e-prescribing system, that met certain government set criteria, you could get an increase in your Medicare payments.

The government also developed safe harbor protections under the anti-kickback statutes[1] and an exception under the Stark statutes[2] that would allow hospitals and other providers to provide hardware and software to physicians at minimal cost to the physician. This was designed to eliminate the regulatory barriers to the adoption of EHR and EPS systems and to promote faster adoption of such systems by physicians.

Finally, as part of the recent government stimulus legislation, more funds were directed at this effort. This has spurred a growth in entities that offer services related to EHRs or EHR systems.

While all of this sounds good, most of the money is not money that comes upfront, nor is it guaranteed money. The physician must make the investment and then meet the bureaucratic (*e.g.*, paperwork) requirements to qualify to get the money, and even then there is no guarantee.

Finally, many believe that the amount of money an individual physician will get will not cover the costs incurred. This means that while there is real pressure to adopt EHRs, there is little incentive at the point of care to do so. From the lab industry's perspective, there are no incentives at all to participate, and the thoughtful laboratory executive will see that there is real potential for the changes that we are in the early stages of to dramatically change the competitive picture in the industry. When there is a challenge to competition in the marketplace, laboratories can be expected to take bigger risks to remain competitive.

Affect on the Current Laboratory Marketplace

Since labs have been using the placement of computers in physician offices as a competitive edge since the early 1990s, it has become somewhat of a standard service that a lab must offer to stay competitive. While it is true that many physicians, particularly smaller practices, do not necessarily want or accept these devices for a variety of reasons, the laboratory that hopes to be competitive in the physician office and reference lab market must have the capability to provide them.

With the advent of EHRs systems, almost all of which will have the capability to order laboratory tests, the standalone laboratory computer will have less and less value as adoption of EHRs spreads. Further, because of the safe harbor and Stark exceptions, labs will not be able to place computer systems in physician offices that do anything more than order tests and receive results without meeting the full requirements of these protections.

In addition, these protections have certain criteria that may make it impossible for physicians to have both the lab computer and the EHR system provided by a hospital in their office at the same time. It does not take much to realize that the advantage will fall to the hospital-based laboratory in the future as far as the value of a computer in the physician's office is concerned.

That said, the compliance risks involved are going to be highest during the transition to EHRs. The protections provided under the safe harbor and Stark exceptions are not well understood by the lab industry or the physician community and are complex. These protections actually consist of four separate pieces of regulation that consist of an e-prescribing component under each law and an EHR component under each law. While they are similar in many respects, they are distinct in a manner that takes into account the technical differences in the two statutes.

I am not going to attempt to address the actual protections in this column, but I am trying to make the point that all laboratory compliance officers need to become familiar with these regulations because as time goes forward compliance issues are going to arise related to them as physicians try to gain the advantages related to them while deferring the costs.

Some Potential Compliance Risks

In many cases, physicians are looking to somehow defer the costs associated with implementation of their EHR while still getting the benefits provided by government incentives and making their practice more marketable to patients. It is here that the compliance risk resides. Labs may be asked why they can provide a computer to a physician for free while the hospital has to charge 15 percent of the cost of the computer or, as an extension of that, why can't the physician just use the lab's free computer for its EHR needs and not pay the hospital.

In other cases, the lab has paid for the interface between its computer and the physician office computer and now the physician wants to use that same interface to transfer information to the hospital or pharmacy system. Another issue that may arise is that the lab gets the benefit of the physician employee entering data that relates to laboratory services but gets no benefit from that, so the lab should either provide an employee to do that or compensate the physician for doing the lab's work.

The laboratory compliance officer is going to have to provide guidance in this area as it specifically relates to the changes brought about by the adoption of EHRs and the incentives directed at physicians to adopt them. Now is the time to prepare by thoroughly understanding the lab's role and how the safe harbor and Stark exceptions apply (or don't apply) to labs, depending on individual circumstance.

Endnotes:

1. Federal Register / Vol. 71, No. 152 / Tuesday, August 8, 2006 / Rules and Regulations; Page 45110.
2. Federal Register / Vol. 71, No. 152 / Tuesday, August 8, 2006 / Rules and Regulations; Page 45140.

Belton

Continued from 16

at the cutting edge to meet pay-for-performance quality targets but also because it can prevent allegations of fraud based on poor quality of care.[21] The link with quality initiatives and pay-for-performance creates a great opportunity for collaboration and integration of efforts for traditionally separate programs. Compliance officers would be wise to capitalize ad address the compliance risks that can arise from quality of care issues.

Conclusion

The current economic crisis has had devastating consequences on many industries, including health care. Some of these have included downsizing and a reduction of workforce; however, with an effective compliance program and the federal government's heightened scrutiny of health care fraud and abuse, opportunities for compliance growth and a compliance officer's role are not diminishing — they are expanding.

Endnotes:

1. Lisa Girion, *Half of Nation's Hospitals Running Losses,* March 2, 2009. Healthcare, Los Angeles, Times.
2. *Ibid.*
3. Rose Dunn, *Improving Cash Flow in a Down Economy*, Journal of AHIMA/March 2009 – 80/3 p. 23.
4. Maurice Gilbert, *Economic Recovery Plan: Restoring Trust Through Ethics and Compliance*, April 6, 2009, www.corporatecomplianceinsights.com/2009/economic-recovery.
5. Alexander F. Brigham & Stefan Linssen, *What Went Wrong Ethically,* Q3-2008 // Ethisphere, p.23, www.eththisphere.com.
6. "Kyocera founder Kazuo Inamoir criticizes U.S. CEO excess", April 19, 2009, www.usatoday.com/money/complancies/management/advice/ 2009-04019-advice-inamoir.
7. Paul McNulty, *Department of Justice's Rising Expectations*, Paul McNulty, Ethisphere, //Q3/2008, p. 80.
8. *"The Board Report" Transformation: A new era in healthcare*, Special Edition-Tax Alert, Winter 2008-2009, Ernst & Young.
9. Pub. L. No. 111-5.
10. "The Stimulus Act and HIPAA: Privacy and Security in a Health IT Environment" Thompson, Health Care Compliance Series, p 1.
11. *Ibid.* p. 3.
12. Richard Kusserow, Enterprise Risk Management: The Next Evolutionary Step in Compliance, Journal of Health Care Compliance, July-August, 2007, p.54.
13. Carroll, R., Guidance to Contributing Authors-Enterprise Risk Management and Risk Domains, August, 2002, San Francisco, California, pp. 1-2.
14. "The Board Report" Transformation: A new era in healthcare, Winter 2008-2009, Ernst & Young, p. 12.
15. *Ibid.*
16. "Revenue Integrity and Data Use", HFMA, October 29, 2008 www.hfma.org/publications/know_newletter/RevIntegData.htm.
17. Robert R. Corrato, MD, MBA *Denial Management Programs can improve the Revenue Cycle, decrease AR*, Managed Healthcare Executive, October, 2003 p. 2.
18. "Clinical Documentation Improvement Program (CDIP) Training Manual , Based on Teaming for Documentation Prepared for and with Catholic Healthcare West (CHW), Presented by Pricewaterhouse Coopers LLP, 2/1/08.
19. Bill Phillips, Stephen Forney, and Buddy Elmore*, 10 Critical Actions to Minimize RAC Recoupment* for Health Leaders Media, February 23, 2009.
20. "Quality of Care and Compliance: Aligning Incentives/Promoting Quality – 2009, Presented by Foley & Lardner LLP, February, 2009.
21. *Ibid*, p. 3.

Hrehor

Continued from 28

Votto, J. National Association of Long-Term Hospitals 2006. Written testimony before the Committee on Ways and Means, Subcommittee on Health, U.S. House of Representatives. 109th Congress, 2nd session, March 15.

20. Bhatia, A.J., Blackstock, S., Nelson, R., and Ng, T. Evolution of Quality Review Programs for Medicare: Quality Assurance to Quality Improvement. *Health Care Financing Review*, 22(1), 2000. The Hospital Payment Monitoring Program (HPMP) was initially implemented as the Payment Error Prevention Program for inpatient PPS services reimbursed under Medicare. The purpose of these programs was to measure, monitor, and reduce the incidence of inpatient PPS improper payments. When the PPS for LTCHs was implemented with medical review under the purview of QIOs, these services came under the purview of the HPMP.
21. Point estimates and variances for short-term acute care claims were weighted by the number of discharges per month of discharge and state as the sample was drawn monthly by state. Point estimates and variances for long-term acute care claims were weighted by the number of discharges per month only as a single, national sample was drawn monthly. This methodology used for the HPMP was deemed adequate to estimate payment error rates and the processes in place to ensure appropriate determinations of error

were deemed adequate by independent review, Government Accountability Office, *Medicare Payment CMS Methodology Adequate to Estimate National Error Rate*, (GAO-06-300), March 2006.

22. Bhatia, A.J., Blackstock, S., Nelson, R., and Ng, T. Evolution of Quality Review Programs for Medicare: Quality Assurance to Quality Improvement. *Health Care Financing Review*, 22(1), 2000. The Hospital Payment Monitoring Program (HPMP) was initially implemented as the Payment Error Prevention Program for inpatient PPS services reimbursed under Medicare. The purpose of these programs was to measure, monitor, and reduce the incidence of inpatient PPS improper payments. When the PPS for LTCHs was implemented with medical review under the purview of QIOs, these services came under the purview of the HPMP.
23. American Hospital Association. *Coding Clinic*. First Quarter, 2008.
24. The Official Guidelines for Coding and Reporting are available at www.cdc.gov/nchs/data/icd9/icdguide.pdf.

For the Record

Continued from 34

sistance of others from either the corporate office or sister facilities.

Snell: What suggestions would you have for those trying to manage a compliance program in a smaller-sized organization? How can they implement an effective compliance program with limited resources?

Tormey: Implementing a compliance program with limited resources requires a "sharp shooters" mentality. You need to limit your focus to the high-risk areas, train employees about how these risks can occur, train them on the consequences, and establish a culture whereby employees feel comfortable reporting suspected misconduct.

The most important thing that a compliance officer in a small facility, probably having additional noncompliance responsibilities, can do is not try and do it all alone. All employees have compliance responsibilities, and I would recommend actively involving department managers to ensure that their employees receive ongoing training and education relating to their responsibilities.

Snell: Who do you turn to when you have a compliance or ethics program management problem? Who in your network helps you when you get stuck?

Tormey: I have an excellent working relationship with our general counsel and one of our external lawyers, who I will consult regarding compliance or ethics management issues.

Snell: What Web sites do you use on a regular basis?

Tormey: I use HCCA, American Health Lawyers Association (AHLA), the Office of Inspector General (OIG), and the Centers for Medicare & Medicaid Services (CMS) on a regular basis.

HIPAA

Continued from 36

counting of disclosures. The presumption is that EHRs contain, or should contain, appropriate technology for easily generating the appropriate accounting of disclosures.

This section, along with section 13403 (b), "Education initiative on uses of health information," which instructs the Department of Health and Human Services to "develop and maintain a multifaceted national education initiative to enhance public transparency regarding the uses of protected health information, including programs to educate individuals about the potential uses of their protected health information, the effects of such uses, and the rights of individuals with respect to such uses," represents an attempt to provide individuals with more information and ultimately more control over how their PHI is being used.

Increased use of HIT systems to create PHI in electronic form also creates new opportunities for individuals to use their PHI in a variety of technology-enhanced ways. Patients can combine information provided by physicians and laboratories with self-created health information in online PHRs; they can carry complete sets of their medical records with them on portable electronic storage devices; they can use various online health care management tools to help them manage their own chronic diseases.

Consequently, section 13405 (e), "Access to certain information in electronic format," is an attempt to make it easier for the individuals to use their own PHI by giving them the right to obtain a copy of protected health information in an electronic format if the covered entity uses an EHR. The individual also can direct the covered entity to transmit the PHI to an entity or person of his or her choice; for example, directly into a PHR or HIE.

On their face, these new provisions appear to be a reasonable attempt to provide increased protections to sensitive health care information, give individuals better tools for accessing and using their own records, and provide them with more control over how their personal health information is used by others. This is a laudable goal and likely will be seen as a step forward provided that the implementation of the rules is not so onerous as to cancel out any potential improvements in effectiveness and efficiency.

Whether or not these provisions achieve the overarching goal of improving the effectiveness and efficiency of the health care system will depend on whether new EHR, HIE, and PHR technologies incorporate the appropriate encryption and auditing technologies and if the rules, recommendations, and guidance documents that map out compliance details adequately consider the cost and other administrative burdens of implementing the new technologies, policies, and procedures required for compliance.

Endnotes:

1. ARRA section 13402(h)(2).
2. CFR 154.528(a)(1)(i).

Settlements

Continued from 38

tial fraud, and "mere billing errors or overpayments…should be submitted directly by the provider to the appropriate claims-processing entity, such as the Medicare contractor." In retrospect, this statement by the OIG foreshadowed the 2009 Open Letter.

2009 Open Letter

The 2009 Open Letter makes two key refinements to the SDP. First, the 2009 Open Letter narrows the scope of the SDP by stating that the OIG no longer will accept disclosure of a matter that involves liability under the Stark law in the absence of a colorable anti-kickback statute violation. Significantly, the Open Letter urges providers not to draw any inferences about the government's approach to enforcement of the Stark law.

Second, the Open Letter establishes a minimum settlement amount intended to better allocate provider and OIG resources. For SDP submissions following the date of the Open Letter that are related to the anti-kickback statute, the OIG will require a minimum $50,000 settlement amount to resolve the matter. According to the Open Letter, this minimum amount is consistent with the OIG's statutory authority to impose a penalty of up to $50,000 for each kickback and an assessment of up to three times the total remuneration.[4] The Open Letter notes that the OIG will continue to analyze the facts and circumstances of each disclosure to determine the appropriate settlement amount consistent with the OIG's practice of generally resolving the matter near the lower end of the damages continuum.

Where Do We Go Now?

The 2009 Open Letter has left many providers wondering what this means on a going forward basis with respect to potential Stark law violations. There are many providers who uncover technical violations of the Stark law in the ordinary course of compliance reviews or other audits. In the past, in an attempt to act ethically and cooperate fully with the OIG, many of these providers self-disclosed these potential violations to the OIG under the SDP. Today, however, without any evidence of an intent to induce referrals, providers no longer are permitted to utilize the SDP.

Interestingly, and ironically, through the 2009 Open Letter's refinements to the SDP, the OIG has limited provider opportunities to work cooperatively with the government and receive lesser penalties and fewer integrity obligations to those providers whose actions were undertaken with the specific intent to induce referrals. Providers who violate the Stark law through no intentional wrongdoing (*i.e.*, without specific intent to violate either the Stark law or the anti-kickback statute), on the other hand, are excluded from this benefit.

In light of the 2009 Open Letter, providers who discover Stark law violations should evaluate seriously the facts surrounding the violation and the decision of whether and to whom to disclose. Seeking acceptance into the SDP by arguing that there is evidence of an anti-kickback statute violation has the potential for significant consequences. Without an accompanying colorable anti-kickback statute violation, however, providers have fewer options with respect to disclosing and resolving Stark law violations.

For example, providers may disclose the matter to the OIG outside of the SDP, but the means for doing so are less clear, and the potential benefits for being forthcoming and cooperative are not guaranteed. Thus, potential risk and liability is greater than under the SDP. Alternatively, following the OIG's guidance in the 2008 Open Letter, providers who determine that the conduct at issue constitutes a mere billing error or overpayment may submit the overpayment directly to the appropriate claims-processing entity, such as the Medicare contractor.

The ability of Medicare contractors to analyze Stark law matters is unclear, however. Furthermore, Medicare contractors likely have no authority to waive the full statutory Stark law damages, thus subjecting providers to potentially draconian penalties. Providers also may disclose matters to their local U.S. attorney's office, but again, it is unclear whether this approach can achieve the benefits generally afforded under the SDP.

Endnotes:

1. 63 Fed. Reg. 58399 (Oct. 30, 1998).
2. *Id.*
3. 63 Fed. Reg. 58399, 58401 (Oct. 30, 1998).
4. 42 U.S.C. § 1320a-7a(a)(7).

Disclosure

Continued from 50

also involve a "colorable anti-kickback statute violation." Further, the OIG advised that for "kickback-related submissions accepted into the SDP..., [and those coupled with Stark law violations], we will require a minimum $50,000 settlement amount to resolve the matter."[3] Thus, with respect to Stark law technical violations, the OIG will no longer accept self disclosures.

It is worth noting that at the present point in time there is no office within either HHS or CMS specifically charged with accepting and resolving self disclosures of potential Stark law technical violations. Before anyone comes to the conclusion that they can ignore the Stark laws, however, keep in mind that CMS continues in its intention to audit hospitals for Stark law compliance.

Pending are plans to survey hospitals on their physician relationships through the Disclosure of Financial Relationships Report (DFRR) to be certified by senior hospital management. These reports are designed to examine financial relationships between hospitals and referring physicians. Should this plan proceed to execution it will place hospitals with improper physician arrangements in a difficult position. As such, hospitals should continue the review of all their physician relationships as part of their auditing and monitoring — not only in connection with the anti-kickback statute but also the Stark laws.

The answer to the question — disclose or not disclose — is to make careful reading of the guidance offered by the OIG. For overpayments and errors that do not suggest violations of the law, SDP is not the answer; instead, it should be brought directly to the attention of the contractor that processes claims. For self-disclosures under the anti-kickback statute, keep in mind that this is a specific intent crime requiring evidence of willful violation. This means that one of the purposes of the arrangement was to provide a flow of benefit in return for expected business. Evidence that this exists requires disclosure. For self disclosures under the Stark law, ensure there is evidence of a "colorable" anti-kickback statute violation.

Endnotes:

1. See 63 Fed. Reg. 58399 (October 30, 1998).
2. See 63 Fed. Reg. at 58400.
3. See www.oig.hhs.gov/fraud/docs/openletter.

Pharmaceutical

Continued from 52

- promotional speaking;
- Phase I-IV clinical trials;
- investigator-initiated research; and
- meals and other nonmonetary items.[7]

Pfizer's announcement has been followed by others offering varying levels of transparency — including Johnson & Johnson's May 7th press release that it would begin to voluntarily disclose payments made to physicians by its U.S. pharmaceutical, medial device, and diagnostic companies.[8] Johnson & Johnson did not provide additional details as to what is included in payment, but its strong public support of the Sunshine Act implies that its initiative likely would take components from the proposed legislation.[9]

IOM Report

The next addition in this succession toward greater transparency was the April 28, 2009, IOM report. As stated by Bernard Lo, chair of the committee that wrote the report, "It is time to end a number of long-accepted practices that create unacceptable conflicts of interest, threaten the integrity of the medical profession, and erode public trust while providing no meaningful benefits to patients or society."[10] The report called on Congress to require pharmaceutical companies (and their foundations) to report, through a public Web site, the payments they make to doctors, researchers, academic health centers, professional societies, patient advocacy groups, and others involved in medicine.

According to the report, a public record of this sort could serve as a deterrent to inappropriate relationships and undue industry influence. Of note is the difference between the Sunshine Act and the IOM report. As noted above, that Act only applies to physicians, physician medical practices, and practice groups. The report asks Congress to require public reporting on payments to researchers, institutions, professional societies, patient advocacy and disease specific groups, and providers of medical education.

Application

As evidenced by the various initiatives impacting transparency, the question is not whether greater transparency of physician relationships will be forthcoming; the question is what impact the required transparency will have on manufacturers, physicians, and consumers. While many, including Grassley, Kohl, and those behind the IOM report, argue that greater transparency inevitably will result in a reduction in the number of conflicts of interest and improve the underlying integrity of the physician-patient relationship, others continue to argue that such broad requirements could result in a hesitation on the part of manufacturers to provide, or physicians to accept, certain forms of payment including professional education. Such groups argue that loss of industry-supported professional education would decrease the quality of continuing medical education

(CME) as well as the opportunity for those serving underserved areas to have access to the high-quality CMEs that are often offered or supported by industry.[11]

Whether through CIAs, legislation, or some other means, the trend toward greater transparency of physician relationships in the pharmaceutical space is not losing steam. The inclusion of disclosures in the recent CIAs, and the latest IOM report in conjunction with the proposed Act, should serve as a wake-up call to manufacturers of all sizes.

The levels of transparency being called for are increasing, and while we do not yet know if the required transparency will take the form of the currently proposed Sunshine Act, or something broader, such as what is called for in the IOM report, it is certain that pharmaceutical manufacturers will be required to provide greater public access to their physician relationships and payments. Accordingly, now is the time for manufacturers to take stock of their existing conflict of interest policies, related training materials for employees, and the processes they have in place to track and audit physician payments so that these entities can be prepared when they are asked to show their hand.

Endnotes:

1. CIA between the OIG and Cephalon, Inc. (Sept. 29, 2008) (Cephalon CIA); CIA between OIG and Eli Lilly and Company (Jan. 14, 2009) (Eli Lilly CIA).
2. Cephalon, *supra* n.2 at Section III.M; Eli Lilly, *supra* n. 3 at Section III.M.
3. *Id.*
4. *Id.*
5. "Covered drug" is defined to include any drug for which payment is available under title XVIII (Medicare) or a state plan under title XIX (Medicaid) or XXI (SCHIP).
6. Pfizer to Publicly Disclose Payments to U.S. Physicians, Healthcare Professionals and Clinical Investigators, Pfizer News, February 9, 2009.
7. *Id.*
8. Johnson & Johnson Announces Support for Kohl-Grassley Physician Payment Sunshine Act of 2009, Johnson & Johnson Press Release (May 9, 2009).
9. *Id.*
10. News from the National Academies, Voluntary and Regulatory Measures Needed to Reduce Conflicts of Interest in Medical Research, Education, and Practice, April 28, 2009.
11. *Transparency Implications on Industry Support for Continuing Medical Education*, Jess Ebert, Pharma Compliance Blogspot, May 7, 2009.

Best Practice

Continued from 54

Risk

Common questions that may help determine if your facility is at high risk due to the lack of a policy on a specific topic or issue include the following:

- Will the policy help improve patient safety or quality of care by describing expectations, standards of practice?
- Is the subject matter a regulatory standard that requires a written policy or specific course of action?
- Is the subject matter a matter of common sense and standard of practice that is found in textbooks?
- Is your policy enforceable?

Do not create policies that you cannot enforce because you are setting yourself up for liability. Make sure you clarify in your policy the meaning of "must" and "should."

References

Last but not least, the policy should have references to support any governing oversight and evidence-based standards. This provides validation for those who are educating and those who are implementing.

Health Information Mgnt.

Continued from 56

5. inappropriate programming or use of "default" code assignments to influence reimbursement; and
6. programming a specific service with two sets of codes to affect payment — for example, the OIG report listed a case in which emergency room physicians were contracted for services by a hospital; the physicians were paid based on code provided to the hospital while the hospital used a different

set of codes for reporting services and kept the higher amount from upcoding.

Well-designed computer-assisted software includes:

1. built-in fraud and abuse detection and prevention tools;
2. interactive informational software that provides reminders and prompts concerning compliance requirements for correct code use and reporting;
3. audit trails that follow the process from source information to code assignment;
4. adherence to all coding conventions and rules; and
5. analytic reports that reveal trends and scores to detect unusual coding patterns that detect fraud or abusive billing practices.

More research is needed to increase the comfort level by the industry in the merits and compliance readiness for additional automation of the coding process. Automated Coding Software: Development and Use to Enhance Anti-Fraud activities provided foundational information in 2005,[5] but the environment has changed. Demands are great for coding accuracy and completeness; we have workforce shortages requiring smart use of knowledge workers and increased productivity to allow us to work smarter toward compliance-ready systems.

Endnotes:

[1] Brown, J, (2000) Medical billing software and processes used to prepare claims, available from oig.hhs.gov/oei/reports/oei-05-99-00100.pdf.

[2] Delving into computer-assisted coding (2004 available fromlibrary.ahima.org/xpedio/groups/public/documents/ahima/bok1_025099.hcsp?dDocName=bok1_025099.

[3] Computer Assisted Coding Of Medical Information Market Shares Strategies, and Forecasts 2008 to 2014 wintergreenresearch.com/reports/computer%20assisted%20coding.htm.

[4] Delving into computer-assisted coding (2004 available fromlibrary.ahima.org/xpedio/groups/public/documents/ahima/bok1_025099.hcsp?dDocName=bok1_025099.

[5] Garvin, J & Watzlaf,V (2005) Automated coding software: development and use to enhance anti-fraud activities available from library.ahima.org/xpedio/groups/public/documents/ahima/bok1_031700.pdf#page%3D1.