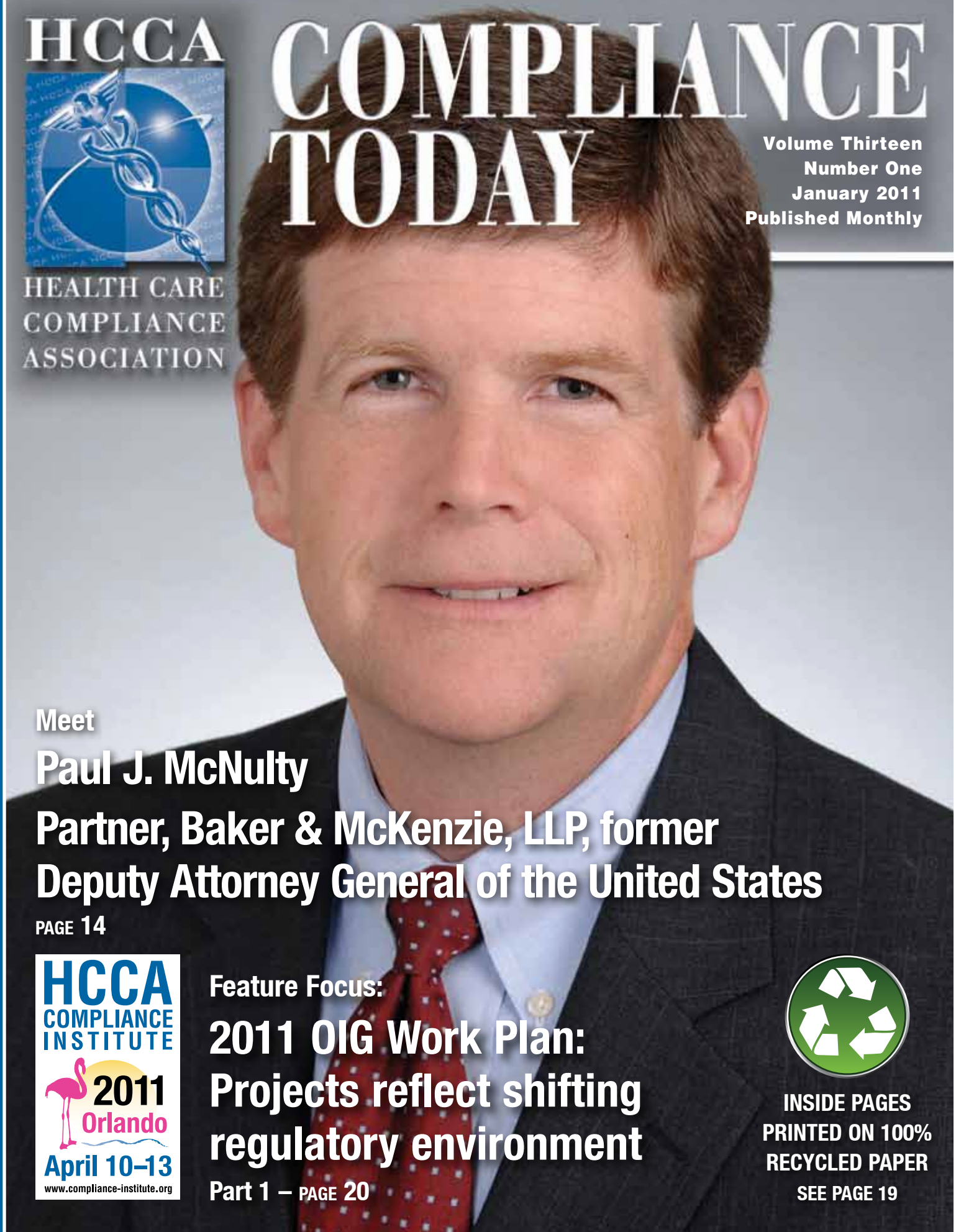
HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY

Volume Thirteen
Number One
January 2011
Published Monthly



Meet

Paul J. McNulty

Partner, Baker & McKenzie, LLP, former Deputy Attorney General of the United States

PAGE 14

Feature Focus:

2011 OIG Work Plan: Projects reflect shifting regulatory environment

Part 1 – PAGE 20

INSIDE PAGES PRINTED ON 100% RECYCLED PAPER

SEE PAGE 19

EARLY BIRD

DEADLINE EXTENDED

Register by or on January 21, 2011, and save $575!

HCCA's 15th Annual **COMPLIANCE INSTITUTE**

April 10–13, 2011 ☀ Orlando, FL

The Walt Disney World Swan and Dolphin Resort

GENERAL SESSION HIGHLIGHTS

AUDREY T. ANDREWS
Chief Compliance Officer
Tenet Healthcare Corporation

JOHN C. FALCETANO
Chief Audit & Compliance Officer
University Health Systems of Eastern Carolina

ODELL GUYTON
Senior Corporate Attorney, Director of Compliance
Microsoft Corporation

DANIEL R. LEVINSON
Inspector General, Office of Inspector General, U.S. Department of Health and Human Services

DAVID B. ORBUCH
Chief Compliance Officer
Ovations

JAMES STEWART
Editor-at-Large, *SmartMoney*; Columnist, *The Wall Street Journal*; Best-Selling Author and Pulitzer Prize Winner

DEBBIE TROKLUS
Assistant Vice President Compliance
University of Louisville HSC

Continuing edication credits are available visit; www.hcca-info.org/ceu for more information.

LEARNING TRACKS INCLUDE:

- General Compliance/Hot Topics
- Long-Term Care
- Privacy & Security
- Physician Compliance
- Legal & Regulatory
- Auditing & Monitoring
- Quality of Care
- Advanced Discussion Group
- Industry Immersion

HCCA COMPLIANCE INSTITUTE 2011 Orlando April 10–13 www.compliance-institute.org

REGISTER AT WWW.COMPLIANCE-INSTITUTE.ORG

Compliance Today (CT) (ISSN 1523-8466) is published by the Health Care Compliance Association (HCCA), 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Periodicals postage-paid at Minneapolis, MN 55435. Postmaster: Send address changes to **Compliance Today**, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435.

INSIDE

CMS issues proposed anti-fraud regulations and voluntary disclosure guidance

By Kimberly Brandt

Editor's note: Kimberly Brandt is Counsel at Alston & Bird LLP in Washington DC. She may be contacted by telephone at 202/239-3647 or by e-mail at kimberly_brandt@alston.com.

On September 23, 2010, the Centers for Medicare and Medicaid Services (CMS) released two key anti-fraud documents: (1) a proposed rule[1] to implement significant anti-fraud provisions of the Patient Protection and Affordable Care Act, as amended by the Health Care and Education Reconciliation Act (collectively, PPACA) that would impact providers and suppliers enrolled in Medicare, Medicaid, and the Children's Health Insurance Program (CHIP); and (2) a guidance document on the CMS Voluntary Self-Referral Disclosure Protocol.

Proposed anti-fraud rule

The proposed rule implementing the anti-fraud provision of PPACA emphasizes fraud prevention and is an attempt to steer CMS away from engaging in "pay and chase" where the agency detects fraud after the fact and then attempts to recoup payments and takes action against the perpetrators. The rule is designed to ensure that only legitimate suppliers and providers with legitimate claims are enrolled in Medicare, Medicaid, and CHIP. The majority of the provisions in the proposed rule would be effective on or after March 23, 2011 and comments on the rule had to be submitted by November 16, 2010.

Under the proposed rule, CMS intends to:

- **Suspend payments to a provider or supplier where a credible allegation of fraud exists.**

In the proposed rule, CMS proposes to define "credible allegation of fraud" as "an allegation from any source, including but not limited to fraud hotline complaints, claims data mining, patterns identified through provider audits, civil false claims cases, and law enforcement investigations." Existing Medicare rules limit the suspension of payments to 180 days (with extensions allowed in certain circumstances), but the proposed rule would eliminate the 180-day time limit in cases where suspensions are based on credible allegations of fraud. PPACA specifies that payments may be suspended unless there is "good cause," which CMS proposes exists where: (1) law enforcement makes specific requests not to suspend payments; (2) CMS determines that beneficiary access to necessary items or services may be jeopardized; (3) CMS determines that other remedies would more effectively or quickly protect Medicare funds; or (4) CMS determines that suspension is not in the best interests of the Medicare program.

Some possible consequences to consider are:

- The inclusion of "fraud hotline complaints" under the definition of "credible evidence of fraud" could create a challenge for compliance officers, because it might have the unintended chilling effect on hotlines if it puts the providers at a greater level of risk for potential government investigation.
- Providers, particularly small entities, might be unable to remain financially viable and need to cease or reduce beneficiary services in cases where payments are suspended based on credible allegations of fraud.

- **Place a temporary moratorium on enrollment.**

Either based on provider type or geographic area or both, an enrollment moratorium would establish the authority to deny providers and suppliers the opportunity to enroll in and bill the Medicare, Medicaid, and CHIP programs when necessary to help prevent or fight fraud, waste and abuse. Under the proposed rule, CMS intends that temporary moratoria on the enrollment of new providers and suppliers in Medicare could be imposed (and extended) in six-month increments when (1) CMS identifies a trend associated with a high risk of fraud, waste, or abuse; (2) a state has imposed a moratorium on enrollment in a particular geographic area and/or on a particular provider or supplier type; or (3) CMS has identified a particular provider or supplier type and/or a particular geographic area that has a high potential for fraud. The enrollment moratoria would be limited to newly enrolling providers and suppliers and establishment of new practice locations (not to a mere change of location).

A possible consequence to consider is that this provision might have an impact on new business ventures in areas which might become subject to a moratoria while a new entity is being created.

- **Screen and classify potential providers as risks.**

CMS wants to strengthen and build on current provider enrollment rules to ensure potential providers and suppliers are appro-

priately screened according to the risk of fraud, waste, and abuse before being allowed to enroll in and bill Medicare, Medicaid, and CHIP. Currently CMS has three categories (low, moderate, and high) for risk of fraud, waste, and abuse. Under the proposed rule, these risk categories are further defined and CMS is given the ability to move a provider or supplier to a higher risk level, based on various factors such as past payment suspension history, Medicaid billing history, etc. For those newly enrolled "high risk" providers, Medicare contractors can use the screening tools utilized in the lower levels of risk in addition to requiring a criminal background check and submission of fingerprints.

- Outline requirements for states to terminate providers from Medicaid and CHIP when terminated by Medicare or another state Medicaid program or CHIP.
- Authorize CMS to terminate providers and suppliers from Medicare when terminated by a state Medicaid program.
- Require institutional providers to pay an application fee.

A fee of $500 would become effective March 23, 2011 and for each subsequent year, as adjusted based on the consumer price index. Providers can request a "hardship" waiver of the fee when submitting applicable applications to Medicare.

- **Solicit input on how best to structure and develop provider compliance plans.**

PPACA now requires compliance plans that will ensure providers are aware of and comply with CMS program requirements. CMS is specifically seeking comment on whether the seven elements of effective compliance and ethics programs, which are included in Chapter 8 of the US Federal Sentencing Guidelines Manual, should serve as the foundation for the core elements.

Something to consider is that all Medicare/Medicaid participating providers and suppliers should be aware of this new requirement and track it closely. It is likely that providers and suppliers who have established compliance programs will need to make changes to comply with the new regulations. Those who do not have a compliance program will need to quickly come into compliance.

CMS voluntary self-referral disclosure protocol

Section 6409 of the PPACA requires the Secretary of Health and Human Services (HHS), along with the Inspector General of HHS, to develop a self-referral disclosure protocol (SRDP)[2] for providers and suppliers to self-disclose violations of the physician self-referral statute.

Highlights from the guidance document and the SRDP include:

- **The SRDP is intended for the disclosure of matters, which in the reasonable assessment of the disclosing party, are actual or potential violations of the physician self-referral law.**

The Office of Inspector General's (OIG) Self-Disclosure Protocol will remain available for all other violations of law, and disclosing parties with Corporate Integrity Agreements or Certification of Compliance Agreements must use the SRDP when making disclosures related to violations of the physician self-referral law and copy the disclosing party's OIG monitor.

Disclosures must be submitted electronically to 1877SRDP@cms.hhs.gov and the original and one copy should be mailed to the Division of Technical Payment Policy, ATTN: Provider and Supplier Self-Disclosure, Centers for Medicare and Medicaid Services, 7500 Security Boulevard, Mailstop C4-25-02, Baltimore, MD 21224.

Disclosures must include a description of the actual or potential violation that includes statements on (1) how the violation was discovered and steps taken to address it and prevent future abuses; (2) past conduct or other enforcement actions against the disclosing party; (3) pre-existing compliance programs and their adequacy as well as the measures taken to restructure the non-compliant relationship or arrangement; and (4) ongoing investigations and whether the disclosing party has knowledge that the violation is already under investigation by a Government agency or contractor.

The disclosures should also include:

- Financial analysis information about (1) the amount (itemized by year) that may be due based on the period of non-compliance by the disclosing party; (2) calculation of the amount; and (3) a summary of auditing activity and key documents that were relied upon.
- A certification signed by the disclosing party's CEO, CFO or other authorized representative stating that, to the best of such individual's knowledge, the information provided on the SDRP is based on a good faith effort by the disclosing party and is truthful.

Upon electronic submission of a violation, CMS will send a response e-mail to acknowledge receipt of the disclosure and then begin verification of the disclosure submission. If CMS requests additional information, the disclosing party will have at least 30 days to furnish such information. Any matters outside the scope of the disclosure may be pursued independently of the SRDP.

Facts and circumstances of each individual violation may be considered in determining whether a reduction of payment is appropriate. Factors that may be considered include:

Continued on page 7

ARE YOU PREPARED FOR THE RAC AUDITOR?

Take control with a strong defense

The RAC Auditors will soon be calling on your hospital. The RAC appeals process is very complex and missed deadlines can result in the automatic recoupment of your legitimate revenues. To minimize your risk of financial losses, you need to be prepared with practical, reliable processes and controls to ensure that critical appeals deadlines are met, with complete, substantiated information.

Compliance 360 is the leader in compliance and risk management solutions for healthcare. More than 300 hospitals nationwide rely on us every day to ensure compliance with legal and industry regulations. Using our unique software solutions, they are always "audit ready" with both proactive defenses and the audit management tools needed to ensure successful audit response and appeals. We are proud to help these healthcare organizations prevent and contain compliance sanctions and we stand ready to help you as well.

To learn more about the Compliance 360 Claims Auditor™ for managing RAC audits, visit www.compliance360.com/RAC or call us at 678-992-0262

Compliance 360®
www.compliance360.com

CMS issues proposed anti-fraud regulations and voluntary disclosure guidance

...continued from page 5

(1) the nature and extent of the improper or illegal practice; (2) the timeliness of the self-disclosure; (3) the cooperation in providing additional information; (4) the litigation risk associated with the disclosed matter; and (5) the disclosing party's financial position.

- Reporting and returning of overpayments must occur by the later of the date which: (1) is 60 days after the overpayment was identified; or (2) any corresponding cost report is due, if applicable. The obligation to return an overpayment within 60 days will be suspended upon the disclosing party's receipt of CMS' confirmation that the disclosure has been received. This suspension will continue until a settlement agreement is entered into, the disclosing party withdraws from the SRDP, or CMS removes the disclosing party from the SRDP.
- If a settlement agreement is entered into as a result of the disclosure, the disclosing party agrees that no appeal rights attach to the claims. Disclosing parties that withdraw or are removed from the SRDP may appeal overpayment demand letters.

Conclusion

As one can see from the two anti-fraud documents summarized above, CMS is very active in this area and providers and suppliers must consider the impact of the proposed rule and SRDP guidance. Although certain aspects of the proposed regulations are dictated by PPACA, CMS has applied its discretion in many respects in the proposed rule and SRDP guidance so that providers and suppliers would be well served to review their compliance programs in areas where this recent guidance would have a significant financial or operational impact. ■

1 75 Fed. Reg. 58204
2 SRDP available online at http://www.cms.gov/PhysiciansSelfReferral/Downloads/6409_SRDP_Protocol.pdf

CCB The Compliance Professional's Certification

The Compliance Certification Board (CCB) compliance certification examinations are available in all 50 states. Join your peers and demonstrate your compliance knowledge by becoming certified today.

The CCB offers certifications in Healthcare Compliance (CHC), Healthcare Research Compliance (CHRC), Healthcare Privacy Compliance (CHPC), and the Certified in Healthcare Compliance Fellowship (CHC-F).

Certification benefits:

- Enhances the credibility of the compliance practitioner
- Establishes professional standards and status for compliance professionals in Healthcare and Healthcare Research
- Heightens the credibility of compliance practitioners and the compliance programs staffed by these certified professionals
- Ensures that each certified practitioner has the knowledge base necessary to perform the compliance function
- Facilitates communication with other industry professionals, such as physicians, government officials and attorneys
- Demonstrates the hard work and dedication necessary to succeed in the compliance field

For more information about certification, please call 888/580-8373, email ccb@hcca-info.org, or visit our website at www.hcca-info.org.

CONGRATULATIONS!! THE FOLLOWING INDIVIDUALS HAVE RECENTLY SUCCESSFULLY COMPLETED THE CHC , CHRC AND CHPC CERTIFICATION EXAM, EARNING THEIR CERTIFICATION:

Rheena M. Abucay
Yvette Bairan
Angelina M. Bolton
Laura Bracis
Stephen C. Buckingham
Linda S. Bugdanowitz
Kara H. Butler
Cathy Cahill
Deborah L. Carlino
Tamie K. Case
Carolyn Cocotas
Linda M. Coleman
Dennis K. Daniels
Lori A. Davis
La Vonda De Witt
Rick Diaz
Russell N. Fail
George A. Fatoush
Kathy L. Gleason
Heidi N. Goodman
Timothy M. Gorton
Alison M. Green
Kim E. Greene
Patricia A. Gregory
Ellen Gutmaker
Michael R. Holper
Mona B. Jackson
Leah L. Kennedy
Robyn Joy Labombarda
Hamid Larijani
Mary L. Legerski
Marshall S. Lieberman
Suliman Limbada
Angela B. Madden
Sherry R. Malusa
Rafael Maristela
Alice H. Martin
Debra L. Martirone
Barbara A. McDonald
Daniel M. McManus
Irma Medel
Donald Lewin Mellman
William August Metcalf
Ciarra R. Miles
Tracy Miller
Karen W. Mulroe
Kristin E. Murphy
Karen E. Murphy
Keith I. Nelson
Peggy A. O'Donovan
Timothy J. Oujiri
Kathleen Owens
Jacki A. Pemrick
Heather R. Piernik
Annmarie P. Rainford
Lynn C. Reno
Amy M. Rhone
Carlos Rios
Mark Rowe
Peiman Saadat
Paula S. Scarton
Susan R. Schneider
Brett L. Shrader
Karen A. Sieverding
Danette L. Slevinski
Susan C. Straumanis
Chad A Sullivan
Deirdre Taylor
Alta S. Whisnant
Michael J. Williamson

Anna Barden
Linda M. Coleman
Stephanie Marie Macholtz
Mary L. Veazie
Gail Mary Walsh
David R. Whiting

Tina M. Adams
Cassandra A. Andrews Jackson
Markus Avery
Carolyn Michele Barton
Jenny M. Bernhard
Andrea L. Britt
Milton R. Burbidge
Cheryl Dekker-Esters
Christine Demarco
Madlyn Dornaus
Charlotte Edwards
Martin L. Edwards
Nayfe S. Faillace
Elizabeth A. Floersheim
Sheila K. Furjanic
Katherine Anne Gorris
Linda S. Heape
Nancy Helmick
Margaret E. Hennings
John A. Hodge
Cheri Huber
Jennifer E. Johnson
Kym K. Keller
Candice M. Kramer
Judy Allums Kuczynski
Janneen M. Lambert
Linda A. Le
Marcia F. Matthias
Dawn P. Morgenstern
Angela Lynn Newberry
Cheryl J. Nikas
Annette Divers Norton
Brandi Periera
Shannon Ladon Perkins
Mary J. Poulson
Sara S. Powers
Mark D. Schutzmann
Craig R. Seacotte
Joy R. Shimabukuro
Roger A. Skinner
Lori J. Strauss
Charles B. Synco
April A. Ten
Tina C. Tolliver
Michael L. Woitkowiak

Protecting the elderly: New reporting requirements for LTC facilities

By Jeannie Adams

Editor's note: Jeannie Adams is a Director in the firm of Hancock, Daniel, Johnson, and Nagle, PC in Richmond, Virginia. She represents hospitals, nursing facilities, hospices, ambulatory surgery centers, physicians, and other licensed healthcare providers in administrative and regulatory matters before state and federal agencies and courts. She may be contacted by e-mail at jadams@hdjn.com.

On March 23, 2010 the Patient Protection and Affordable Care Act of 2010 (PPACA)[1] was enacted as a major health reform package. PPACA established many new requirements that apply to long-term care (LTC) facilities.

Encompassed within PPACA is the Elder Justice Act of 2009 (EJA), which amends Title XI of the Social Security Act (SSA)[2] and became effective immediately upon enactment. This federal response to the needs of the elderly was timely, because the proportion of the United States population age 60 years or older is drastically increasing with the large number of Baby Boomers approaching retirement and old age. Sadly, it is estimated that each year, anywhere between 500,000 and 5,000,000 elders in the United States are abused, neglected, or exploited. The EJA is the first comprehensive national legislation enacted on elder abuse. It has the overall legislative purpose of detecting, preventing, and prosecuting elder abuse, neglect, and exploitation.

The EJA adds several new elder justice provisions and requirements specific to long-term care providers. For example, included in the EJA are opportunities to receive federal grant money available to improve staff training programs and overall quality of care. Facilities may be eligible to receive federal funding to train and retain employees, improve the workplace environment and culture, and update workplace technology. In addition, a significant provision of the EJA mandates implementation of enhanced reporting requirements for crimes that occur with in LTC facilities receiving over $10,000 in federal funding. Outlined below are the key reporting features required for compliance with these new, more stringent standards.

Increased reporting requirements

Although LTC facilities receiving federal reimbursement through Medicare or Medicaid are already bound by a set of reporting requirements, the EJA reporting requirements are more expansive.

The EJA reporting provision requires:

- Reporting of "any" reasonable suspicion of a crime against any facility resident or individual who receives care from the facility.
- The report must be made to both the HHS Secretary and one or more law enforcement entities, including police, sheriffs, detectives, public safety officers, corrections personnel, prosecutors, medical examiners, investigators, and coroners.
- The report must be made within two hours if the suspected crime resulted in serious bodily injury or within 24 hours if it did not.
- Individuals who are owners, operators, employees, managers, agents, or contractors of the LTC facility are covered by the provision.
- Failure to report a suspicion can result in individually assessed fines up to $200,000 to $300,000 if the failure to report

exacerbates the harm to the victim or another individual, and exclusion from the Medicare and Medicaid programs.
- If a facility employs a covered individual who has been excluded by the HHS Secretary from participating in any federal health care program for violating the reporting requirements of the EJA, the facility itself becomes ineligible to receive federal funds under the Social Security Act.
- LTC facilities can be fined up to $200,000 for retaliation against an employee who makes a legitimate report of suspected abuse, and may be excluded from receiving federal funding in the future.
- LTC facilities must conspicuously post a notice of employee rights that includes information on how to file complaints for retaliation by the facility for reporting under the EJA.
- The HHS Secretary has authority to take into account the financial burden on providers with "underserved populations" in determining penalties.

Staying in compliance

Step 1: Determine if your facility is receiving federal funds in excess of $10,000. If so:
- Inform all employees of the new EJA reporting requirements;
- Review current policies and notify all employees and covered individuals who have an obligation to report;
- Develop protocols for the process of reporting; and
- Post a notice of employee rights regarding retaliation within the facility.

Step 2: Train all employees on key elements in the EJA reporting provision that distinguish it from the CMS reporting requirements already in place. The EJA:
- Requires reporting of any crime, rather than just abuse, neglect, and misappropriation of property;
- Specifically enumerates covered individuals who must file a report, rather than merely imposing the obligation on the facility;
- Does not specify that the crime must be an act of staff misconduct, and therefore can apply to the reporting of resident-on-resident abuse or abuse by a third party; and
- May require reporting within a strict two-hour time frame.

Step 3: Facilities governed by multiple reporting requirements should follow the strictest provisions, if there are areas in which the requirements differ.

Conclusion

For more than 20 years, Congress has been presented with facts and testimony calling for a coordinated federal effort to combat elder abuse, neglect, and exploitation. Differences in state laws and practices in the areas of elder justice cause significant disparities in prevention, protective and social services, treatment systems, and law enforcement, and lead to other inequities in health care settings and LTC facilities. The enactment of the EJA is the culmination of a federal response to adequately and comprehensively address the issues of elder abuse, neglect, and exploitation.

Many of the details of how the EJA will affect LTC facilities await clarification as the HHS Secretary begins to promulgate regulations to enforce PPACA. What is still unclear from the EJA will begin to develop over the next few years; for example, PPACA does not define the term "reasonable suspicion" of abuse, or what qualifies as a "conspicuous" way to post a notice of employee rights and obligations. To remain in compliance, facilities should interpret the new regulations in the strictest manner.

As the national legislative landscape focuses more attention on elder justice, through increased funding to adult protective services, surveillance programs, forensic detection of crime, and governmental advisory boards, long-term care facilities would be wise to constantly focus on improving the quality of care provided to their residents. Successful long-term care facilities will be those that become leaders in the community with regard to providing high quality care and having zero tolerance for elder abuse. ■

1. The Patient Protection and Affordability Care Act (PPACA). Public Law111-148, H.R. 3590 (2010).
2. 42 U.S.C.S. §1397(j) (2010). Social Security amendment at Section 6703(b)(3).

Be Sure to Get Your CHC CEUs

Articles related to the quiz in this issue of **Compliance Today**:
- **Protecting the elderly: New reporting requirements for LTC facilities**—By Jeannie Adams, page 8
- **Are global surgical packages all encompassing?**—By Melissa Morales and Amanda Gorman, page 28
- **Employment references: Name, rank, serial number. . . Is that all there is?**—By Natalie Wyatt-Brown, page 39

To obtain one CEU per quiz, go to **www.hcca-info.org/quiz** and select a quiz. Fill in your contact information and take the quiz online. Or, print and fax the completed form to CCB at 952/988-0146, or mail it to CCB at HCCA, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Questions? Please call 888/580-8373.

Compliance Today readers taking the CEU quiz have ONE YEAR from the published date of the CEU article to submit their completed quiz.

CMS' Physician Quality Reporting Initiative: From a financial incentive to a quality program

By Joseph T. Cooke, MD and Mary Koval, RN, CPHQ

Editor's note: Joseph T. Cooke is Chief Quality & Patient Safety Officer and Associate professor at Weill Cornell Medical College/Physician Organization located in New York City. Dr. Cooke may be contacted by telephone at 212/746-7498 or by e-mail at jcooke@med.cornell.edu.

Mary Koval is Clinical Quality Program Manager with Weill Cornell Physician Organization and Weill Cornell Medical College/NewYork-Presbyterian Hospital in New York City. Ms. Koval may be contacted by telephone at 646/962-2226 or by e-mail at mak2006@med.cornell.edu.

The Centers for Medicare and Medicaid Services (CMS) instituted the Physician Quality Reporting Initiative (PQRI) in July 2007. Like many other institutions, the Weill Cornell Medical College Physician Organization (WCMC PO), which is comprised of approximately 800 physicians across all specialties, was interested in the financial incentive offered for successful completion of the program. Although there was a concern that the process changes needed for reporting the performance measures would result in lost productivity (thus negating any financial incentive), the PQRI program was viewed as an opportunity to document the excellent quality of care rendered at this organization.

This article will review the successes and challenges we have encountered in implementing the PQRI program across the several health care delivery processes such as patient care delivery, billing, and compliance as we navigated from the PQRI program toward the establishment of performance measures within the organization.

It is no longer acceptable to simply state that an organization provides excellent quality of care. The federal government, insurance payers, and consumers all require proof that excellent care is delivered, which is proved by the reporting of performance measures and the demonstration good patient outcomes. This transparency in the way health care is delivered will be the norm as evidenced by the ARRA HITECH Act[1] which contains provisions to develop health information technology (HIT) standards and policy. Two committees will be formed, called the HIT Standards Committee and HIT Policy Committee. Included in the bill was a provision to define "meaningful use." The PQRI program proves to be a "training ground" for organizations to move toward this end.

The participation in the PQRI program drove us to review many processes in our health care delivery system, beginning with the coding and billing process.

At the WCMC PO, it is the physician's responsibility to assign the appropriate ICD-9 and CPT codes[2] for the services rendered. Certified professional coders are not widespread among the organization, but some specialty departments, such as the surgical sub-specialties, do utilize these coders. Even in these instances, the responsibility of code selection lies with the physician. Accurate coding is assured through a program of prospective audits and physician education conducted by our organization's Billing Compliance staff.

We asked each clinical department to choose at least three PQRI measures to report and track throughout the year. Many departments elected to report on more than three to enhance their chances of successfully reporting three measures in 80% of the applicable cases. These PQRI quality codes were added to the code dictionary in the electronic medical record (EMR), the billing system, and to paper charge tickets. The assignment of the appropriate quality code became an additional responsibility for the physician.

Awareness of the PQRI program and knowledge of the measure criteria by the physician was crucial to ensure the correct quality code was assigned and submitted in all applicable cases. We developed a reporting mechanism to provide timely feedback to the physician on all measure opportunities. An overt decision was made to report PQRI quality codes through a claims-based process via our electronic billing system. The billing system became our data source for the monthly physician reports. The report included the number of opportunities to report a given measure, the percent of opportunities in which the measure was reported, and whether the physician was "successful" in reporting any three measures year-to-date. Extensive physician education, both individual and group, was conducted to increase awareness of the PQRI financial incentive reporting requirement and

the chosen measure criteria. The individual physician education was driven by the prospective billing compliance audits and the analysis of missed reporting opportunities provided by monthly reports. Rolled up departmental reports were presented to the chief medical officer and departmental chairmen at the WCMC PO monthly Operating Board meeting.

A low reporting success rate our first year of implementation drove us to re-visit the physician quality coding process. Using physician feedback and the analysis of missed PQRI reporting opportunities, we revised the selection of the type and number of performance measures and the manner in which the quality codes associated with the measures would be assigned. The PQRI measures were re-selected to ensure that the measures accurately reflected the physician's practice and that the measures would address the process of care provided to improve patient outcomes. The automation of selected measures in the EMR, based on discrete data fields, was investigated to relieve the physician of that responsibility.

A collaborative effort between the organization's Quality Team and the departmental Quality Team was utilized to re-select the PQRI performance measures. Individual physician feedback was solicited and current quality improvement projects, whether existing or planned, were also considered. The PQRI performance measures that were proven to lead to improved outcomes, such as Hb A1C control in diabetic patients, were chosen as well as the preventive measures, such as screening mammography.

The number of measures for each department was reduced to three common measures that are tracked across the organization, plus one specialty-specific measure. The three measures included tobacco inquiry, medication review, and the use of the EMR. By reducing the number of measures and choosing performance measures which were vetted by the physicians, the reporting success increased dramatically.

To decrease the physician workload, the responsibility of selecting the quality codes was removed from the physician. Certain measures were fully automated in the EMR, driven by the completion of discrete data fields. These included tobacco inquiry, the use of the EMR, influenza vaccinations, and medication review. Other measures, such as Hb A1C and screening mammography, depended on the inclusion of laboratory or radiology results entered in the EMR. The measures, in which the measure criterion was more complicated, such as spirometry in chronic obstructive pulmonary disease (COPD) patients, were semi-automated in the system. For the semi-automated measures, the physician was "alerted" when a patient met the criteria and a series of questions followed.

Based on the input by the physician, a quality code was assigned. All fully automated PQRI quality codes were appended to the billing form when the encounter was closed. The semi-automated PQRI quality codes were appended to the billing form only if the physician completed the measure questions.

The physicians saw the automation of select measures as a great advantage, but the accuracy of the quality codes depended on the completion of discrete data fields and the inclusion of radiology and laboratory results.

The monthly reports were revised to include the percent of claims in which a quality code was submitted to indicate the measure was performed appropriately. An analysis of the data showed the physician behavior and practices had changed, but we still had a lower performance rate than expected. A manual review of encounters showed the measure was indeed performed and documented, but in a free text or dictated form, rather than the completion of the discrete data fields. The semi-automated measure quality codes were proven to be accurate, because these codes were dependent on the completion of the measure questions by the physician. The documentation issues were immediately relayed to the physicians, along with education, both individual and group.

Another limitation identified with the implementation of the fully automated codes was found in those measures that allowed for a patient, system, or medical reason for why the measure was not performed, such as in the case of screening mammography. The system allowed only for a "yes, performed" or "no, not performed – reason unspecified" to be entered. For example, on manual chart review, there was clear documentation on why a screening mammography was not done, yet the physician did not get "credit" for performing the measure. The automation of these codes is currently being reviewed to allow for these exceptions. While this is reviewed, some departments have elected to set up a billing edit to stop a claim until a manual chart review can be conducted.

An analysis of missed opportunities, despite the automation of select measures, revealed that education among the billing staff, data entry staff, and coders was required to familiarize this staff with the measure criteria and the quality codes. In many instances, the missed opportunity was a result of the code not being entered into the billing system, because the staff was unsure of its meaning. Billing staff training was also required to ensure that the quality codes did not split off from the office service code claim, thus rendering the quality code invalid. In addition to the staff education, edits were created which would hold a claim if the PQRI quality code was missing on an applicable encounter. These encounters were reviewed by the billing staff and the appropriate

Continued on page 13

 ...continued from page 11

quality code was added to the claim after consulting with the physician. All departments were encouraged to take advantage of the direct charge interface between the EMR and the billing system, because this would effectively eliminate any omission error by the billing staff.

Quality codes were omitted on the claim in some instances, despite the staff education and system checks. For this reason, we are moving towards registry reporting. An added advantage of registry reporting is that it enables the physician to correct the data prior to submission, thus ensuring the accuracy of the codes. The accuracy of the quality codes submitted is not only important for quality improvement initiatives, but it is imperative in order to comply with the False Claims Act.

The accuracy of the submitted PQRI quality codes has not yet been subject to scrutiny by CMS. Early this year, Quality Insights of Pennsylvania was contracted by CMS to conduct a random review of the accuracy of the submitted quality codes. Our introduction letter clearly stated that this was not an audit and no penalty would be levied, but that this was an exercise to determine the reliability and validity of the PQRI program. Our accuracy rate for this review was excellent. The measures that were most problematic in terms of accuracy were those measures that were fully automated and allowed for a patient, system, or medical reason for why the measure was not performed (i.e., screening mammography as described above). The request for records was forwarded with no further communication from Quality Insights of Pennsylvania. We have not had any further requests for records from either CMS or their designee.

The selection of the PQRI quality codes, regardless if automated by the EMR or chosen by the physician, is reviewed for accuracy via the prospective billing compliance review process and the analysis of monthly reports. Physician feedback is provided when an issue has been identified and corrective action taken, if needed.

Finally, the means by which we deliver health care to our patients was reviewed. Practice processes, including the use/non-use of ancillary personnel such as medical assistants, was reviewed by each department. To ease the administrative burden of the physician, responsibilities were added to the front office/registration staff and medical assistants. These additional responsibilities include, but are not limited to, ensuring that the patient brings a complete list of their medications with dosages and entering the current list in the medical record, documenting the tobacco status in the appropriate data field, and entering the patient's pharmacy information in order to electronically submit a prescription to the pharmacy. Many departments elected to increase the use of medical assistants to help with the documentation of the performance measures.

At the end of 2010, we expect the PQRI reporting success rate via claims submission to be at about 80%. This is a substantial improvement from the 2009 success rate of 39%. The major factors contributing to the reporting success include our regular physician and administrative staff education regarding the PQRI program and the form of monthly meetings, the collaboration with the Information Technology team, timely feedback of success rates, the monthly analysis of missed reporting opportunities, and the involvement of the Billing Compliance Office. To ensure success in 2011, registry reporting will be utilized in lieu of claims-based reporting.

The type and accuracy of chosen performance measurements should be closely evaluated as we prepare for the transition from a volume-based, non-reporting delivery of health care to quality-based health care with measurement and transparency. The research conducted thus far on the reliability and validity of quality measures extracted from the EMR does not yet offer any concrete conclusions[3] and further research is certain to be conducted in this field. In the meantime, the type of performance[4] measure and the number of measures reported should be evaluated closely. At a minimum, the performance measures chosen should ultimately improve patient outcomes, can be easily and accurately extracted from the EMR, and include nationally accepted measures. Most importantly, the measures chosen should include physician involvement and support, portray the practice accurately, and allow for continuous quality improvement with in a practice.

We are on the cusp of a new type of health care delivery system which is certain to improve the quality of care to our patients. The participation in the incentive programs, such as PQRI and Meaningful Use, will enable us to determine which performance measures and reporting processes work best within the organization to ensure compliance with all regulatory bodies and to ensure that accurate and complete physician data is submitted prior to public publication. Most importantly, successful participation will provide the physician with the data needed to improve the quality and the value of the care delivered. ■

Acknowledgements: Our thanks to Adam Cheriff, MD, Chief Medical Information Officer; Aurelio Gracia, Associate Director, Electronic Medical Record; and Brian Tuckman, Business Reporting Manager for their help in preparing this article.

1 American Recovery and Reinvestment Act (ARRA, P.L. 111-5), and the Health Information Technology for Economic and Clinical Health Act (the HITECH Act). Both were signed into law in February 2009.
2 The International Classification of Diseases (ICD), 9th edition. Clinical Research Terminology (CRT)
3 Kitty S. Chan, Jinnet B. Fowles, Jonathan P. Weiner: Electronic Health Records and the Reliability and Validity of Quality Measures: A review of the Literature. *Medical Care Research and Review*; Sept. 2010, 67(5): 503-27
4 Chassin MR, Loeb JM, Schmaltz SP, Wachter RM: Accountability measures—using measurement to promote quality improvement. *New England Journal of Medicine*, 2010 Aug, 12;363(7):683-8

feature article

Meet Paul J. McNulty

Partner, Baker & McKenzie, LLP, former Deputy Attorney General of the United States

Editor's note: Rebecca Walker is a Partner at the law form of Kaplan and Walker LLP in Santa Monica, California and Princeton, New Jersey. She is a member of the Advisory Board of SCCE and is the author of Conflicts of Interest in Business and the Professions: Law and Compliance, *published by Thomson West. She may be contacted by e-mail at rwalker@kaplanwalker.com.*

Paul McNulty may be contacted in Washington DC at paul.mcnulty@bakermckenzie.com.

RW: Can you tell our readers a little about your background?

PM: Sure. I've spent most of my legal career in public service, and I've been blessed with some wonderful opportunities. I began my legal career on Capitol Hill and served a total of eleven years as a House staffer, mostly as a counsel with the House Judiciary Committee. As Chief Counsel to the Crime Subcommittee, I was involved in the drafting of a wide range of criminal laws and procedures, which provided a great foundation for my work as a prosecutor and defense lawyer. I also served for nine years at the Department of Justice in various roles, including Director of Policy and Communications, Principal Associate Deputy Attorney General, US Attorney for the Eastern District of Virginia, and finally Deputy Attorney General. I was confirmed by the Senate for the US Attorney job three days after the attacks on 9/11, and this was the dominant focus of my four-year tenure in that position.

RW: What are some of the responsibilities of a Deputy Attorney General?

PM: The DAG is the Chief Operating Officer of the Department of Justice [DOJ]. With more than 100,000 employees and 40 components, including the FBI [Federal Bureau of Investigations], DEA [Drug Enforcement Agency], and US Attorneys, DOJ is an extraordinary management challenge. The job involves a great deal of problem-solving on issues of policy, operations, and case-specific issues. I spent much of my time attending White House national security meetings with the deputies of other agencies, resolving policy disputes, hearing from companies that were appealing prosecution decisions, and working on the Department's budget. The aftermath of the 9/11 attacks has made the job far more difficult.

RW: You are perhaps best known in the Compliance and Ethics community as the author of the McNulty Memo, which provided instructions to federal prosecutors regarding the factors they must consider in determining whether to charge an

organization for alleged criminal conduct. The McNulty Memo, now incorporated into the US Attorneys' Manual, instructs prosecutors to consider, among other things, an organization's compliance program. Can you provide any insight into how prosecutors consider compliance programs in the charging decision?

PM: I think it's fair to say that compliance programs come into play in prosecutions mostly as a mitigating factor. The common scenario is that a company negotiating with the government about an issue of misconduct will offer a presentation on its compliance program to demonstrate that it has a strong ethical culture

and has taken concrete steps to avoid wrong-doing. The company's goal is to reduce the penalty for its failure. We are also seeing government attorneys, who are now more familiar with compliance programs, increasingly ask about compliance programs in order to determine whether the company failed to act responsibly and establish appropriate controls.

RW: Do prosecutors consider compliance programs for more than just whether or not to charge the organization? For example, could a robust program be a factor in a decision as to exactly what to charge an organization for, or for other parts of a charging decision?
PM: Well, first I would like to see more prosecutors take the Department's guidelines seriously and give compliance appropriate consideration in charging decisions. The history has been that "cooperation credit" is far more significant than "compliance credit." If the government fails to recognize substantial compliance efforts in its prosecution decisions, it will eventually discourage companies from investing in robust compliance programs. It's possible that an impressive compliance presentation could convince the government to forego certain charges and focus instead on less serious issues, or it could make the difference between a civil (e.g., SEC) resolution versus a criminal charge.

RW: Do you have any advice for our readers regarding how best to incorporate the various factors discussed in the McNulty Memo into their own compliance programs?
PM: I would suggest two ideas. First, get on top of the compliance issue before something goes wrong. The Memo refers to "pre-existing" compliance and, if there is any hope of getting real compliance credit with the government, a strong program will need to be already in place. And second, be prepared to respond quickly and effectively to a credible allegation of misconduct. A lot of companies ignore or deny problems when they first arise, and that can undermine an argument to the government later on that genuine remedial efforts have been made (another Memo factor). It also may be advisable to self-report, which is a case-by-case decision. A slow response will delay that opportunity, and that could be critical if a whistleblower beats the company to the disclosure punch. Every company should have a plan in place to ensure that it will take the right steps in response to ethical violations.

RW: What types of documents are most critical to "proving up" a program to a prosecutor?
PM: There are several types of documents and written materials that are necessary for making an effective compliance presentation. Let me suggest five buckets of materials. First, evidence of leadership commitment to a strong compliance culture and program, including communications to employees and board of directors engagement; second, risk assessments; third, policies and procedures, such as manuals and standard due diligence controls; fourth, training materials; and fifth, monitoring and auditing efforts.

RW: As you know, the revisions to the Federal Sentencing Guidelines became effective on November 1. What do you think the impact of the board reporting provision might be?
PM: It seems to me that boards are steadily becoming more engaged in compliance activities. There is more board training, and compliance officers are having more contact with audit committees and board oversight. Therefore, I don't think the amendment to the Sentencing Guidelines will make much of a difference. It's a rare circumstance when the wrong-doing involves top management, and that's what the amendment is addressing. When serious allegations of this nature arise, the board usually steps in and directs the internal investigation, a response which should satisfy the revised Guidelines. Of greater concern to me is the provision which requires self-reporting in order for a company to get a downward departure under the Guidelines when the misconduct involves senior management. There are many imaginable situations in which the government may learn about a problem independent from a company's disclosure, but that doesn't mean the company's compliance program is ineffective.

RW: What about the impact of the new Application Note regarding organizations' response to misconduct?
PM: The biggest impact may be the requirement that companies review their compliance programs for gaps or weaknesses in the wake of significant violations. I see companies doing this now, when they are getting ready to show their programs to the government, but it's often not a part of a company's general response to a problem. In the future, companies may need to have a clear record of compliance enhancements in order to get credit for having an effective compliance program.

RW: With the OECD's[1] Good Practice Guidance for Anti-Bribery Compliance Programs and the UK Bribery Act Adequate Procedures Guidance, we have seen a lot of movement regarding compliance and ethics programs on the international front. What do you think will be the impact of the OECD's Good Practice Guidance?
PM: In the U.S., I think we will see prosecutors, over time, with a more global perspective on compliance. I urge my clients now not to be too focused on the Sentencing Guidelines, as if it's the only pronouncement on the issue of compliance best practices. Certainly if a business organization is the subject of a sentencing calculation by a federal judge, the Sentencing Guidelines are the relevant standard. But, since the vast majority

Continued on page 17

of corporate prosecutions end in a pre-charge settlement, prosecutors may operate with a wider perspective in their assessment of compliance programs. DOJ's Fraud Section attorneys are familiar with the OECD guidance, and they are tracking the development of the U.K. Bribery Act. They will expect companies to be on top of the compliance challenge. Outside of the U.S., the OECD's efforts in holding companies more accountable for their anti-corruption enforcement, combined with their good practices guidance, will result in more attention to compliance by international companies.

RW: What about the impact of the UK's Adequate Procedures Guidance?

PM: It looks as though the U.K. is going to use broad principles in its guidance, which gives companies more flexibility in complying with what is expected. An interesting question is whether they will expect more when determining if a company had "adequate procedures" for preventing corruption. The new law creates a strict liability offense for companies when persons associated with them engage in corruption, and the "adequate procedures" defense is the way companies can avoid this liability. There will be a big outcry if this defense is more difficult to achieve than the guidance seems to indicate.

RW: In your experience, what are some of the most important attributes of an effective compliance and ethics program?

PM: Controls are very important. By this I mean practical mechanisms for ensuring compliance with ethical standards. Having too many procedures can be a problem, but there must be a balanced approach that includes appropriate tools. Another key element is oversight. This may be the weakest part of most compliance programs. In addition to regular audits, companies should find ways to ensure employees are following the program's requirements, especially in high-risk jurisdictions. And, of course, leadership is critical. The stronger the compliance message is, the stronger the compliance program.

RW: Given your extensive experience in anti-bribery compliance, can you provide our readers with some practical advice on the implementation of effective anti-bribery compliance programs?

PM: In addition to what I've already said about key compliance elements, I would say that the most important part of an anti-bribery compliance program is managing third parties in high-risk jurisdictions. Use of agents, consultants, distributors, and other third parties in countries with low CPI scores[2] is fraught with risk. And, the government is showing an interest in pushing "willful blindness" cases, meaning cases where the company should have known that a third party was paying a bribe, but it purposely avoided having actual knowledge. Global businesses should maintain an inventory of all their third parties, but certainly those in high risk places.

Also, we shouldn't forget joint ventures. These relationships are also very risky from a corruption perspective. Putting the necessary policies and procedures in place is not difficult, and effective training is something most companies have learned to do quite well. Therefore, asking the right questions and setting up sensible protocols is especially important. Up until now, most of the companies that have gotten into trouble under the Foreign Corrupt Practices Act had clearly inadequate compliance programs when the misconduct was occurring. Now that so much is being done to strengthen compliance programs, it will be interesting to see how DOJ and the SEC will weigh pre-existing compliance against a one-off violation. That's where this issue is going. ■

1 Organisation for Economic Cooperation and Development
2 Transparency International's Corruption Perception Index.

Letter from the CEO

If you have any questions that you would like Roy to answer in future columns, please e-mail them to: roy.snell@corporatecompliance.org.

Rory Jaffe

In a recent article, I made an "inside" joke that about three people laughed at. That's assuming everyone who knew what I was joking about laughed. The rest of the readers may have come away from "the joke" thinking that Rory Jaffe doesn't support strong and effective compliance programs. Just to be sure that no one is left in doubt, Dr. Jaffe is one of the most effective compliance professionals ever to practice in our profession. He supports a strong and effective approach to compliance with the law, company policy, and ethical behavior.

Learning the elements of an effective compliance program is very, very easy. Implementing a compliance program is a little harder. Implementing an effective compliance program is really hard. Achieving what Rory did as a compliance officer is the equivalent of finding the Holy Grail.

"Learning the elements of an effective compliance program is very, very easy. Implementing a compliance program is a little harder. Implementing an effective compliance program is really hard. Achieving what Rory did as a compliance officer is the equivalent of finding the Holy Grail."

The hardest part of this job is knowing when to let something go and when to throw yourself in front of the bus. And when you throw yourself in front of the bus, you have to know how to do it in a way that the bus stops inches from your nose. That is accomplished through years of experience negotiating, collaborating, compromising, and debating with very powerful people. Many people freeze or give up too easily. Rory has got this part of the job down pat. He believes that a strong compliance program is important and he knows how to do it without sounding like Chicken Little.

Some people run up and down the halls of their organization screaming, "The sky is falling!," every time a problem is found. They have little regard for the size of the problem. They want to fix every problem instantly, and they want to do it with a Louisville Slugger. Rory tosses Nurf Balls at Nurf Ball problems and stands his ground when necessary. He also worries about the culture.

He tries to affect the culture. He understands that it is not an exact science, and it is a difficult thing to change. However, he appreciates the value of one of the most effective tools in a compliance professionals arsenal, establishing an ethical culture. Although I agree with Rory, I choose not to beat this drum because there are many people beating it, and many are implying it's all you need. That said, any compliance professional who doesn't do everything they can to affect the culture is missing a very important point.

And, Rory is a very nice guy. In fact, this summer a pig fell out of a truck right in front of his car. Rory caught the pig and put it in his car. They he raced after the truck to get the pig back to the owner. A policeman stopped him and said, "Where are you going in such a hurry and why is that pig in the car?" Rory told him and the policeman said, "Slow down, you will never catch the truck now. Why don't you take the pig to the zoo or something?" Three hours later the same policeman stopped Rory for speeding again and said, "Why are you speeding again, and I thought I told you to take that pig to the Zoo?" Rory said, "I did, and we had so much fun we are going out for dinner." ■

Social Networking

Editor's note: John Falcetano, CHC-F, CCEP-F, CHRC, CHPC, CIA is Chief Audit/Compliance Officer for University Health Systems of Eastern Carolina and Treasurer of the HCCA Board of Directors. John may be contacted by e-mail at jfalcetano@uhseast.com.

Welcome to the Social Networking column. This column is devoted to providing our members with a list of topics being discussed this month on the Health Care Compliance Association's (HCCA) social networking site. The social networking site is where our members can find answers to their questions and network with other members online.

The HCCA social networking website functions like any other online community that shares common interests. The site has multiple communities that members can access.

Two of the great benefits available for members are the social networking library and member discussion groups. Here is an example of a white paper from the document library and a discussion topic being discussed by the Auditing and Monitoring Discussion Group:

Document Library:

A white paper that discusses ten things organizations could do to enhance internal whistleblowing in light of the Security Exchange Commission's whistleblower awards under the Dodd-Frank Act. The white paper provides a practical approach that focus on the legal issues.

Discussion Topic:

Ongoing discussions concerning changes to the Federal Sentencing Guidelines, such as providing incentives for the compliance officer to report to the board.

I encourage everyone to become involved with the Social Network, it is a great way to participate in the discussion, review the comments, or just talk with your peers. You can access the social networking site by going to the following link: www.hcca-info.org/sn ■

feature focus

2011 OIG Work Plan: Projects reflect shifting regulatory environment, Part 1

By Sara Kay Wheeler, Esq. and Stephanie L. Fuller, Esq.

Editor's note: Sara Kay Wheeler is a Partner in King & Spalding's Healthcare Practice Group and works with its Special Matters Group. She has extensive experience in the creation and implementation of corporate compliance programs and investigations, government contractor audits, voluntary disclosure strategies, clinical research compliance, and managed care arrangements. Ms. Wheeler also defends health care providers who are investigated by federal and state enforcement entities. Ms. Wheeler is currently serving on the HCCA Board of Directors. She may be contacted by phone at 404/572-4685 or by e-mail at skwheeler@kslaw.com.

Stephanie L. Fuller is an Attorney in King & Spalding's Healthcare Practice Group. She represents health care clients in government investigations, internal investigations, and complex business disputes. In addition, she advises clients on federal and state regulatory issues, including Medicare and Medicaid reimbursement, compliance, fraud and abuse, and Stark Law compliance. She may be reached by phone at 404/572-4629 or by e-mail at sfuller@kslaw.com.

On October 1, 2010, the Department of Health and Human Services (HHS) Office of Inspector General (OIG) released its Fiscal Year (FY) 2011 Work Plan.[1] The OIG Work Plan is a prospective summary of the investigative, enforcement, and compliance activities that will be initiated or continued in the coming year. Over the years, the OIG Work Plan has become an important compliance resource used by providers and suppliers participating in federal health care programs to guide compliance efforts.

OIG has provided Work Plans on its website for every year dating back to FY1997.[2] The OIG Work Plan has always been viewed as a useful resource for providers and suppliers to guide compliance efforts, but the rapidly changing regulatory environment may prove to make the 2011 OIG Work Plan more valuable to providers and suppliers than in past years.

The mission of the OIG is to ensure the integrity of federal health care programs by detecting and preventing fraud, waste, and abuse. To further its mission, OIG audits, inspects, and investigates many aspects of federal health care programs, and the Work Plan addresses the OIG's efforts to combat fraud, waste, and abuse.

Recurring themes

The focus of the OIG Work Plan changes slightly from year to year, but recurring themes appear throughout the Work Plan each year. These recurring themes include: quality, reimbursement methodologies and utilization, and the Centers for Medicare and Medicaid Services (CMS) and state oversight initiatives, particularly through the use of government contractors.

Quality

One of the primary missions of the OIG is to protect the health and welfare of beneficiaries who participate in federal health care programs. The 2011 OIG Work Plan contains many reviews focused on improving the quality of care delivered to beneficiaries and ensuring that such beneficiaries are receiving care that will not harm them. As described in more detail below, the OIG will continue its review of a number of quality-of-care issues in 2011, including trends in hospital readmissions and reporting of adverse events.

Updating reimbursement methodologies

OIG has identified several areas for which it will review reimbursement methodologies and recommend updates, as warranted. OIG's stated goals in these endeavors are to realign the payment methodology with true costs of service and to reduce incentives, where they exist, for over-utilization based on favorable reimbursement.

Review of CMS and State oversight initiatives

The role of government contractors with respect to Medicare and Medicaid program administration and oversight has greatly expanded over the past several years. The effectiveness (or perceived ineffectiveness)

of government contractors has also garnered attention recently.[3] The 2011 Work Plan outlines several efforts focused on assisting the agencies and the contractors with performing their functions more effectively.

The Patient Protection and Affordable Care Act of 2010 (PPACA),[4] as amended by the Health Care and Education Reconciliation Act of 2010 (Healthcare Reform Law),[5] has further introduced significant change to the regulatory environment. For example, while the voluntary pursuit of compliant practices and procedures has been considered best practice in the health care industry for decades, PPACA transformed the regulatory landscape by mandating that hospitals and other health care providers maintain compliance programs as a condition of enrollment in the Medicare and Medicaid programs.[6] With the inclusion of mandatory compliance requirements in PPACA, it is apparent that government expectations are significantly increasing with respect to the sophistication and execution of compliance programs in the health care industry. Consequently, the 2011 OIG Work Plan also includes several projects or activities that address these new PPACA requirements. PPACA's changes include, but are not limited to, the following.

Reimbursement

- Home health restrictions for Medicare and Medicaid
  - Providers must document that a face-to-face encounter between the provider and the patient occurred within a reasonable period of time as determined HHS for Part A, and during the 6-month period prior to certifying eligibility (or other reasonable period determined by HHS) for Part B.
- DME restrictions for Medicare and Medicaid
  - Providers must document that a face-to-face encounter with the patient occurred during the 6-month period prior to certifying eligibility (or other reasonable period determined by HHS).

Sunshine Provisions

- By March 31, 2013, a manufacturer that provides a "payment or other transfer of value" to a "covered recipient" (or to any entity or individual at the request of a "covered recipient") during calendar year 2012, must report certain information to HHS regarding those payments and other transfers of value.
- Manufacturers must report payments and other transfers of value to "covered recipients" which are defined as:
  - Teaching hospitals
  - Physicians (except physicians who are employees of the applicable manufacturer)

Enforcement

- PPACA provides HHS with the authority to withhold payments due to a "credible allegation" of fraud.[7]
- A violation of the Anti-kickback Statute has been made an explicit False Claims Act violation as well.[8]
- PPACA expands the types of conduct subject to civil monetary penalties.[9] The expanded types of conduct include:
  - failing to provide timely access to OIG for audits ($15,000 per day);
  - knowingly making, using, or causing to be made or used a false record or statement material to a false claim ($50,000);
  - knowingly making a false statement on an enrollment application, bid, or contract ($50,000); or
  - ordering or prescribing services (lab tests, drugs, durable medical equipment) during a period in which the person ordering has been excluded ($50,000).
- PPACA authorizes penalties for Medicare Advantage and Medicare Part D Plans that:
  - enroll individuals in a plan without prior consent;
  - transfer an enrolled individual from one plan to another without prior consent, or solely to earn a commission;
  - fail to comply with marketing restrictions regarding approval of marketing materials and prohibited marketing activities;
  - employ or contract with an individual or entity who engages in the above activities; or
  - misrepresent or falsify information.

Compliance

- Compliance programs will be mandatory for certain providers.[10]
- Nursing home facilities must implement compliance and ethics programs.[11]

Program Integrity

- Drug manufactures and distributors must report to HHS the identity and quantity of drug samples requested and distributed.
- State Medicaid programs are required to comply with provider and supplier screening, oversight, disclosure, moratorium, and compliance requirements.
- Nursing home facilities must also implement quality assurance and performance improvement programs.

Oversight

- RAC Program expanded to Medicaid, Medicare Part C, and Medicare Part D.[12]
  - Medicaid
    - Interface between Medicaid RACs and MICs is currently unknown.
    - States may contract with multiple Medicaid RACs.

Continued on page 22

 ...continued from page 21

- Medicare Parts C and D
  - RACs will review the effectiveness of anti-fraud plans of Part C and Part D contractors.
  - Program begins by December 31, 2010.
- Enhanced oversight of new providers and suppliers for up to one year after enrollment. Enhanced oversight may include:
  - Prepayment review
  - Payment caps
  - With respect to DME suppliers, HHS may withhold payment for 90 days from the first submission of a claim.

The remainder of this article aims to provide a high-level overview of the OIG's priorities by provider and supplier type. Many of the projects highlighted in the 2011 Work Plan and summarized in this article reflect changes introduced in PPACA and other significant regulatory and political developments. Part II (in our February 2011 issue) will highlight other areas of focus for OIG, including Medicare Advantage, Medicare Part D, Medicaid CMS and state oversight activities.

OIG's focus by provider/supplier type

OIG recognizes that some compliance risk areas apply to specified provider or supplier types. Accordingly, below is an overview of significant OIG priorities by provider and supplier type.[13]

Hospitals

As a result of the changing regulatory environment, compliance risk areas for hospitals continue to expand in scope and complexity. Within the hospital setting, numerous risk areas exist, given the variety of health care professionals, the high volume of varied claim types, and the complexities of hospital reimbursement. Specifically, these hospital risk areas often include, but are not limited to, quality of care, reimbursement and billing, physician relationships, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Stark Law,[14] the federal Anti-kickback Statute,[15] and the Emergency Medical Treatment and Active Labor Act (EMTALA).[16] The hospital-specific reviews in the FY2011 OIG Work Plan include several quality-of-care reviews, including hospital readmissions and adverse events.

Hospital inpatient outlier payments

Noting that outlier payments represented about 5% of Medicare inpatient payments (approximately $6 billion in 2009), OIG will examine Medicare outlier payment trends nationally to identify characteristics of hospitals with high or increasing rates of outlier payments. OIG also noted that recent whistleblower lawsuits have resulted in millions of dollars in settlements from hospitals that allegedly inflated Medicare claims to qualify for outlier payments. (Section I, page 8, Work in Progress)

Hospital readmissions

OIG will continue to review Medicare claims to evaluate trends in the number of hospital readmissions. OIG will also assess the extent of CMS's oversight of such hospital readmissions. (Section I, page 5, Work in Progress)

Observation services during outpatient visits

OIG will continue to review Medicare Part B payments for outpatient observation services. OIG will also evaluate whether and to what extent a hospital's use of observation services affects the care Medicare Beneficiaries receive and their ability to pay out-of-pocket expenses for such services. (Section I, page 8, New Start)

Hospital reporting for adverse events

OIG will review the type of information hospitals' internal incident-reporting systems capture. Additionally, the OIG will review data collected pursuant to a 2010 OIG study to determine the extent to which hospital incident-reporting systems captured adverse events and reported such events to external patient safety oversight entities. (Section I, page 6, Work in Progress)

Medicare excessive payments

OIG will review Medicare claims with high payments to determine whether the payments are appropriate and the effectiveness of the claims processing edits used to identify excessive payments. OIG suggests that unusually high payments may be incorrect for various reasons. Pursuant to the Claims Processing Manual (Publ. No. 100-04. 4, § 20.4), hospitals are required to report units of service as the number of times that a service or procedure was performed. Accordingly, OIG will review certain outpatient claims in which payment exceeded charges and selected Healthcare Common Procedure Coding System (HCPCS) codes for abnormal billings. (Section I, page 3, Work in Progress)

Critical Access Hospitals

OIG will continue to evaluate payments to critical access hospitals. OIG will also assess whether critical access hospitals have met the critical access hospital designation criteria and other conditions of participation described in 42 CFR, Part 485, Subpart F. (Section I, page 2, Work in Progress)

Home health agencies, nursing homes, and hospice

Beneficiaries of services provided by home health agencies (HHAs), nursing homes, and hospice represent a vulnerable segment of the population. Accordingly, OIG will continue to focus on quality initiatives in this segment of the industry. With regard to HHAs, OIG will scrutinize payments to HHAs, given the substantial increase in HHA payments over the years. OIG will also review hospice utilization in nursing homes,

because a recent OIG report concluded that a significant percentage of hospice patients in nursing facilities did not satisfy Medicare coverage requirements. OIG will undertake the following specific projects.

Oversight of home health agency data

HHAs are required to conduct comprehensive patient assessments that include Outcome and Assessment Information Set (OASIS) data. The OASIS data reflects the HHAs' performance in assisting patients to regain or maintain their ability to function and perform activities of daily living. The HHAs are required to submit OASIS data to CMS, and CMS uses the OASIS data to compute HHAs' prospective payment rates. OIG will continue to review CMS's process for requiring HHAs to submit accurate and comprehensive OASIS data. (Section I, page 9, Work in Progress)

Home health Prospective Payment System controls

Noting that payments to HHAs have increased substantially over the years, from $8.5 billion in 2000 to $16.4 billion in 2008, OIG will review compliance with various aspects of the home health PPS, including billings for the appropriate location of services provided. OIG will also analyze HHA trends, including the number of HHA claims submitted to Medicare, the number of visits provided to beneficiaries, arrangements with other facilities, and certain ownership information. (Section I, page 9, New Start)

Background checks for long-term care employees

Section 6201 of PPACA requires the Health and Human Services (HHS) Secretary to implement a nationwide program to identify efficient and effective procedures for long-term care facilities or providers to conduct background checks on employees who have direct access to patients. Pursuant to § 6201 of PPACA, OIG will evaluate this program in 2011. (Section I, page 12, Work in Progress)

Medicare Part A payments to skilled nursing facilities

OIG will continue to review the extent to which payments to skilled nursing facilities (SNFs) meet Medicare coverage requirements and will review claims to determine whether claims were medically necessary, sufficiently documented, and coded correctly during calendar year 2009. For payment purposes, beneficiaries are grouped, based on care and resource needs. These groups are referred to as Resource Utilization Groups (RUGs). OIG notes in the Work Plan that a previous report found that 26 percent of claims reflected RUGs that were not supported by the patients' medical records. (Section I, page 10, Work in Progress)

Criminal background checks for nursing facility employees

Noting that nursing facilities that participate in the Medicare and Medicaid programs are required to maintain the dignity and well-being of all nursing home residents, OIG will continue to review whether nursing facilities have employed individuals who have criminal convictions. OIG will then categorize the types of crimes (assuming that OIG finds nursing facilities that employed individuals with criminal backgrounds) for which nursing facility employees have been convicted. OIG will also determine the number of states that require criminal background checks prior to hiring a nursing home employee. (Section I, page 12, Work in Progress)

Hospice utilization in nursing facilities

Noting that an OIG report[17] found that 82 percent of hospice claims for beneficiaries in nursing facilities did not meet coverage requirements, OIG will review Medicare Part A hospice claims and data from the Minimum Data Set (MDS) to describe hospice utilization in nursing facilities. Specifically, OIG will review characteristics of nursing facilities with high utilization patterns of Medicare hospice care and the characteristics of the hospices serving such facilities. OIG will also review the business relationships between nursing facilities and hospices associated with high utilization patterns. (Section I, page 13, Work in Progress)

Durable medical equipment

The 2011 OIG Work Plan includes reviews of several durable medical equipment (DME) issues, including supplier enrollment and monitoring, cost containment measures, the competitive bidding program, medical necessity and frequency of replacement supplies, and suppliers' documentation to support claims for Medicare reimbursement. OIG also continues its efforts to identify fraud and abuse in the wheelchair industry.

Frequency of replacement supplies

OIG will asses the compliance of suppliers of durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS) with Medicare requirements for frequently replaced DME supplies. The Medicare Program Integrity Manual (Publ. 100-08, ch. 5, §§ 2.3 and 5.9) provides that the order or Certificate of Medical Necessity specify the type of supplies needed and the frequency at which the supplies must be replaced, used, or consumed. OIG will select a sample of claims for frequently replaced supplies to determine whether payments to DME suppliers satisfied Medicare requirements. (Section I, page 22, New Start)

Medicare payments for power wheelchairs

OIG continues its efforts to review documentation for payments to DME suppliers for standard and complex rehabilitation power wheelchairs to determine whether the claims were medically necessary. Specifically, OIG will assess whether suppliers had adequate documentation from the beneficiaries' medical records to support the medical

Continued on page 24

...continued from page 23

necessity for a power wheelchair and whether the documentation was consistent with documentation from the physician who ordered the power wheelchair. (Section I, page 22, Work in Progress)

Competitive bidding

Pursuant to §1847 of the Social Security Act, CMS is required to establish a competitive bidding process for the purchase of certain DME supplies. OIG will review DME claims to determine the extent to which suppliers participating in the competitive bidding program are soliciting physicians and influencing them to prescribe certain brands or modes of delivery of covered items that are more profitable to suppliers. In addition, OIG will review billing patterns to identify any changes resulting from the competitive bidding program. (Section I, page 24, New Start)

Other providers and suppliers

Other 2011 Work Plan initiatives are focused on certain categories of providers and suppliers.

Payments for services ordered or referred by excluded providers

OIG will review the extent to which Medicare paid for services ordered or referred by excluded providers. OIG will also examine CMS's mechanisms to identify and prevent improper payments for services based on orders or referrals by excluded providers. (Section I, page 20, New Start)

Error-prone providers: Medicare Part A and Part B

In an apparent effort to hold providers accountable for compliance, OIG will review Medicare Part A and Part B claims submitted by error-prone providers. Specifically, OIG will conduct a medical review on a sample of claims to determine the validity, project its results to each provider's population of claims, and request refunds on projected overpayments. (Section I, page 21, New Start)

Place-of-service errors

Noting that federal regulations at 42 CFR §414.32 provide for different levels of payment to physicians, depending on where services are performed, OIG will review physician coding of place of service on Medicare Part B claims for services performed in ambulatory surgical centers (ASC). Medicare physician payment tends to be higher when the service is performed in a non-facility setting, such as the physician's office. Specifically, OIG will review whether physicians appropriately coded the place of service on claims for services provided in ASCs and hospital outpatient departments. (Section I, page 14, Work in Progress)

Coding of Evaluation and Management (E&M) services

Noting that in 2009, Medicare paid $25 billion for E&M services (19 percent of all Medicare Part B payments), OIG will continue to review

E&M claims to identify trends in the coding for E&M services. Specifically, OIG will review E&M claims to determine whether coding patterns vary by certain provider characteristics. (Section I, page 14, Work in Progress)

Outpatient physical therapy services provided by independent therapists

Reasoning that previous OIG work has identified claims for therapy services by independent physical therapists that were not reasonable, medically necessary, or properly documented, OIG will review outpatient physical therapy services provided by independent therapists to determine whether they satisfy Medicare reimbursement regulations. Specifically, OIG will focus on independent therapists with a high utilization rate for outpatient physical therapy services and determine whether the services satisfied Medicare requirements. (Section I, page 16, New Start)

Polysomnography

Noting that Medicare payments for polysomnography increased from $62 million in 2001 to $235 million in 2009, and coverage was recently expanded, OIG will review the appropriateness of Medicare payments for sleep studies. OIG will also study the factors contributing to the rise in Medicare payments for sleep studies. (Section I, page 17, New Start)

Error rate oversight

Noting that the Comprehensive Error Rate Testing (CERT) program's national estimated improper payments for FY2009 were $24.1 billion (a 7.8 percent error rate),[18] OIG will review certain aspects of the CERT program to evaluate CMS's efforts to ensure accuracy of the FY2010 error rate and to reduce improper payments. (Section I, page 21, New Start) ■

Part 2 will appear in the February issue.

1 The OIG 2011 Work Plan is available on the OIG website at, http://oig.hhs.gov/publications/workplan/2011/FY11_WorkPlan-All.pdf.
2 OIG Work Plans are available on the OIG website for fiscal years 1997 through 2010 at, http://www.oig.hhs.gov/publications/workplan.asp.
3 Letter from Sen. Charles Grassley to CMS Administrator Donald Berwick, M.D., October 6, 2010, available at http://grassley.senate.gov/about/upload/2010-10-15-Letter-to-CMS.pdf.; Letter from Sen. Charles Grassley to CMS Administrator Donald Berwick, M.D., October 15, 2010, available at http://grassley.senate.gov/about/upload/2010-10-15-Letter-to-CMS.pdf.; Letter from Sen. Charles Grassley to CMS Administrator Donald Berwick, M.D., October 29, 2010, available at http://finance.senate.gov/newsroom/ranking/download/?id=75ab598e-fc6d-4eb2-9277-de216f13afc6.
4 PPACA, Pub. Law No. 111-148 (2010).
5 Pub. Law No. 111-152, 124 Stat. 1029 to 124 Stat. 1084 (2010).
6 Pub. Law No. 111-148 § 6401 (2010).
7 PPACA, Pub. Law No. 111-148 §§ 6401(a)(3) and 6402(h)(1) (2010).
8 PPACA, Pub. Law No. 111-148 § 6402(f) (2010).
9 PPACA, Pub. Law No. 111-148 §§ 6402 and 6408.
10 PPACA, Pub. Law No. 111-148 § 6401.
11 PPACA, Pub. Law No. 111-148 §§ 6102, 6111, 6112.
12 PPACA, Pub. Law No. 111-148 § 6411
13 Descriptions in this section of the article are not designed to be exhaustive.
14 42 U.S.C. § 1395nn.
15 42 U.S.C. § 1320a-7b(b).
16 42 USC § 1395dd.
17 OIG: Medicare Hospice Care for Beneficiaries in Nursing Facilities: Compliance with Medicare Coverage Requirements, publ #OEI-02-06-00221. Available at http://oig.hhs.gov/oei/reports/oei-02-06-00221.pdf.
18 The November 2009 Medicare FFS Improper Payments Report is available at https://www.cms.gov/CERT/Downloads/CERT_Report.pdf.

Department of Justice spearheads nationwide implantable cardiac device investigation

By: Frank E. Sheeder and Lindsey F. Bartula

Editor's note: Frank E. Sheeder is a Partner and Lindsey F. Bartula is an Associate in the Dallas office of Jones Day. Frank Sheeder also serves as First Vice President of the Health Care Compliance Association. He may be contacted by e-mail at fesheeder@jonesday.com and Ms. Bartula may be contacted by e-mail at lfbartula@jonesday.com.

The Department of Justice (DOJ) is conducting an ongoing, multi-state, multi-provider investigation into billing compliance relating to hospitals' provision of implantable cardioverter defibrillators (ICDs) and related devices. An ICD is a small electronic device installed inside the chest to prevent sudden death from cardiac arrest due to life-threatening, abnormally fast heart rhythms (tachycardias).

As part of the investigative process, DOJ previously issued extensive Civil Investigative Demands (CIDs) to hospitals around the country. It is notable that the CIDs were not limited to claims to government payers, but covered all payers. Medicare reimbursement to a hospital for ICD implantation is generally in the $40,000 to $50,000 range.

The DOJ is now pursuing a new approach by notifying health care institutions of the government's concerns regarding ICDs billing compliance and extending an invitation to engage in a discussion of the issues. A key area of interest is the timing of the ICD implantation. Medicare does not cover implantation of ICDs in patients who lack a history of arrhythmia if the implantation occurred within a certain period after specific cardiac events or procedures.

As a secondary matter, Recovery Audit Contractors (RACs) have identified implantation and interventional cardiology diagnosis-related group (DRGs) codes as issues for review, and the Office of the Inspector General (OIG) has issued subpoenas related to these devices. It will be important to identify and coordinate activities that are occurring in other contexts in relation to these devices and related services.

The following is a general summary of the prior investigative process, including specific areas of focus and recent CMS developments that illustrate the nature of the information that the government has been seeking from hospitals.

Time line for implantation of an ICD

The DOJ is investigating whether hospitals are compliant with Medicare's National Coverage Determination (NCD) for ICD implantation, including whether hospitals billed Medicare for ICDs for patients whose conditions did not satisfy the coverage criteria set forth in the NCD. In particular, the DOJ is looking at the implantation of an ICD following other cardiac events or procedures. The most recent applicable NCD provides that Medicare does not cover implantation of ICDs in patients who lack a history of arrhythmia if the implantation occurred within three months of a bypass graft or a coronary angioplasty, or within 40 days of an acute myocardial infarction (MI).

CMS maintained this restriction on coverage despite comments that the requirements should not apply to patients who already met the criteria for ICD implantation prior to their most recent event or procedure. Citing the results of a randomized trial to determine whether an ICD will reduce the risk of death in patients who have a recent MI or other conditions, CMS stated that "ICDs have not been shown to improve health outcomes when implanted in patients within 40 days of an [acute MI] and may, in some instances, be harmful in these patients."[1] A few of the interrogatories in the CIDs (discussed below) specifically address hospitals' interpretation of, and compliance with, this restriction on coverage.

New Medicare Claims Processing Manual sections

Health care providers should be aware of the new Medicare Claims Processing Manual (MCPM) sections for implantable automatic defibrillator services. On July 2, 2010, CMS released Transmittal 1994, which implements the new sections, effective as of August 31, 2010.

The new sections address claims processing and coding requirements for ICDs and billing requirements for patients enrolled in a data collection system (DCS). Medicare requires that patients who receive an ICD for the

primary prevention of sudden cardiac arrest be enrolled in a qualifying DCS, and that modifier 'Q0' be used to identify patients whose data is being submitted to a DCS. New Section 270, regarding claims processing, directly references Section 20.4 of the NCD Manual for a complete list of the coverage requirements.

Scope of investigation

The CIDs sent to hospitals by the DOJ provide insight into the nature of the information that the government has been seeking from hospitals. The CIDs are broad requests for information, including extensive document requests and interrogatories that are difficult to answer. The information requests are related to hospital compliance with the ICD implantation NCD. Manufacturers of ICDs have also reported that they are being investigated.

The request for documents can involve a vast amount of information, including, for example, all documents relating to coding, billing, payment, reimbursement, denials of payment, and appeals related to ICDs by all payers, including government, self, insurance, or other private entities. The request may ask for all internal NCD compliance policies and procedures, as well as all documents related to attempts made to determine whether a procedure involving the ICD was covered by Medicare, either before or after the ICD was implanted.

The interrogatories may ask, for example, for an explanation of the timing of ICD implantation. Under the NCD, in certain circumstances providers must wait for a triggering condition before ICD implantation. Additionally, some NCD conditions require that certain events not happen within a period prior to ICD implantation. For example, the NCD requires that in most cases the patient must not have had an acute MI within the past 40 days. An interrogatory may ask for an explanation as to why it would be medically necessary to implant the ICD within 30 days of when a patient had an acute MI and whether Medicare would cover it.

Additionally, RACs have identified implantation and interventional cardiology DRGs as issues for review in all four regions, Regions A through D. The DRG codes at issue in these regions are 222 to 227, involving cardiac defibrillator implant. Region A most recently added cardiology DRGs as issues for review, identifying DRG codes 222 to 227 as approved issues on August 24, 2010.

Finally, the OIG has issued subpoenas to device manufacturers requesting production of documents relating to ICDs. These subpoenas include requests for such information as:

- revenue, sales, marketing and promotional documents;
- documents relating to device reimbursement communications to customers;
- documents relating to scientific studies and registries pertaining to the devices; and
- documents relating to payments or items of value provided to customers.

Recommendation for providers

Establish and maintain attorney-client and work product protection on these issues. The risks here are much higher than they are for other documentation, coding, and billing issues – even the matters such as kyphoplasty and Q codes that are being handled by local Assistant U.S. Attorneys in conjunction with OIG. Proper direction by counsel is a must in this situation. Also, because the reimbursement amounts associated with ICD implantation are in the mid-5 figures, there are significant financial impact concerns.

Engage counsel for a coordinated, efficient, and consistent approach to addressing these issues. This is not a routine matter and it should not be handled through general RAC readiness processes. The risks of generating material that could be used against you, in the process of trying to assess compliance, are simply too high. Much of the work can and should be done inside, but it will need to be done subject to a thoughtful, detailed, and intentional work plan developed in conjunction with counsel.

Promptly validate that all current billing practices are in accordance with the NCD and that all current bills are correct before they go out. If indicated, do a retrospective study to validate whether past approaches have been compliant.

Engage in compliance follow-up, auditing, monitoring, education, and other proactive approaches. Consider whether some of these processes should be done subject to attorney-client privilege and work product protection, given the nature of this issue and the potential exposure. ■

1 CMS: Decision Memo for Implantable Defibrillators (CAG-00157R3). Available at http://www.cms.gov/mcd/viewdecisionmemo.asp?from2=viewdecisionmemo.asp&id=148.&.

Are global surgical packages all encompassing?

By Melissa Morales and Amanda Gorman

Editor's note: Melissa Morales is a Consultant with Healthcare Industries, PricewaterhouseCoopers in the San Francisco office. She may be contacted by e-mail at Melissa.Morales@us.pwc.com.

Amanda Gorman is a Consultant with Healthcare Industries, PricewaterhouseCoopers in the Boston office. She may be contacted by e-mail at Amanda.Gorman@us.pwc.com.

Are all evaluation and management (E&M) services considered part of the global surgical package? What services are actually billable? Some may even wonder what is considered a global surgical package. Resources are available online that can help you decipher the nuances of billing during global periods. In addition to the resources available, there are various steps an organization can take to understand the intricacies of the global surgical package. This will help ensure that your organization is not at risk for inappropriate reporting of E&M services during post-operative periods.

A global surgical package consists of the necessary services performed by the provider in the pre-operative, intra-operative, and post-operative phases of treatment.

Global surgical packages do not encompass all services that may occur during a post-operative period. Discerning which services to include in the global package and which to exclude can be a challenge for every organization. Potential issues arise when the policies concerning global surgical packages are not understood, which can lead to increased compliance risks and ultimately affect provider reimbursement.

Several components comprise the global surgical package. A key component is to identify the length of the global period for each procedure performed. This information can be found in the Medicare Fee Schedule Database (MFSDB) on the Centers for Medicare and Medicaid Services (CMS) website.[1] Post-operative periods applicable to each surgical procedure are outlined in this database by various indicators, such as 0, 10, and 90 days, as well as other non-numerical indicators.

Procedures are subject to surgical provisions classified as minor or major surgeries. The difference in the major or minor classification is reflected in the number of post-operative days assigned to each procedure. Procedures with a global period of 0 and 10 days are considered to be minor, whereas those designated by 90 post-operative days are considered major surgical procedures.

Understanding the global period assigned to each procedure is key, because this will establish the allowance for the normal pre- and post-operative care associated with the procedure. Services included in the global package can be provided in any setting such as, hospitals, ambulatory surgery centers (ASCs), and physician offices. These services include:

- Pre-operative visits performed on the day of surgery for minor procedures; pre-operative visits the day of or the day before major surgery for major procedures.
- Intra-operative services normally included in the surgical period
- Complications following surgery related to surgery, excluding return to operating room
- Post-surgical pain management when performed by the surgeon
- Supplies (with some exclusions)
- Miscellaneous services, including dressing changes; removal of operating pack; local incision care; removal of sutures, staples, wires, tubes, drains, catheters, splints, routine peripheral intravenous lines, or nasogastric and rectal tubes; and changes and removal of tracheostomy tubes
- Post-operative follow-up visits during the identified global period that are related to the recovery from the surgery

Although several services are included in the surgical package, there are a number of items that can be billed and paid for separately. These services include:

- The initial evaluation of the problem by the surgeon (This applies only to major procedures, because the initial evaluation is included in the surgical package for minor procedures.)
- Non–transfer-of-care services provided by other physicians
- Visits unrelated to the surgery
- Added course of treatment
- Diagnostic tests and procedures
- Surgical procedures performed during the post-operative period that are not treatment or re-operations of the original procedure
- Post-operative complications that require a return trip to the Operating Room
- Extensive procedure required when a lesser procedure failed
- Immunosuppressive therapy for organ transplants; and
- Critical care

Understanding the intricacies of included and non-included services will enable your organization to bill and be reimbursed appropriately for the work performed. Organizations often

fail to report services that are not part of the global surgical package, thereby losing out on potential revenue. On the flip side, it's not uncommon for organizations to report E&M services related to the procedure during the postoperative period when the global days are not tracked appropriately. Knowing what is and is not included—and when—prevents potentially obtaining revenue for services that were already allotted for in the procedure. It's important to understand the global period day allotment for procedures and what service is being provided, as well as having proper documentation to support billing any additional services.

You may be asking why this is important. For 2010, the Office of Inspector General (OIG) outlined their intent to "review industry practices related to the number of E&M services provided by physicians and reimbursed as part of the global surgery fee"[2] in the FY2010 Work Plan. This was also listed in their FY2009 Work Plan as an area of concern. Separately billing for E&M visits that are included in the post-operative global surgical period can leave your organization vulnerable to scrutiny and audits by the OIG.

However, keep in mind that not all E&M encounters are included in the global surgical package. If a patient is seen during the post-operative period for a problem that is unrelated to the reason for surgery, this visit can and should be billed. When reporting these encounters, modifier 24 should be appended to the E&M code to advise the payer that this service is unrelated to the surgery performed. It is important to have supporting documentation in the medical record that clearly states the reason for the visit and a documented diagnosis relating to the unrelated problem to support the services reported. However, the misuse of modifier 24 can cause overpayment for services that are considered part of the global surgical package. The intention of modifier 24 is to identify unrelated E&M services provided during the post-operative period by the same physician, but it is often misused to report post-operative complications and related visits.

Determining whether the service is unrelated or not, can be a gray area and a challenge for some organizations. Questions that you would need to think about when considering billing for an unrelated E&M visit during postoperative periods are:

- What is the reason for the patient's visit?
- Were complications from the procedure previously performed treated during this encounter?
- Is the visit related to the procedure the patient had?
- What is the diagnosis outcome of this encounter?
- Is the diagnosis different from the patient's post-operative diagnosis?

Going through this series of questions can guide you to whether or not the E&M service you are about to report is applicable and if modifier 24 should be applied.

Because the OIG has focused on industry standards relating to the number of E&M services provided during post-operative periods and overpayment of these services, organizations need to have measures in place to prevent potential compliance issues. What can be done?

First, reviews of E&M services reported with modifier 24 should be part of your auditing and monitoring process. The method in which you identify encounters to be audited will need to be carefully selected and analyzed to identify potential issues with claim submission and that all providers who perform procedures are reviewed in a timely and consistent manner. In addition, individual departments may want to develop a method for tracking the global days for patients, either in the patient's medical record or through the scheduling system, to give the physicians a reminder on the post-operative follow up time frame.

Second, if your organization has a claim scrubber as part of the billing process, the modifier 24 edit built into the scrubber should be reviewed to ensure that the edit isn't built to automatically append modifier 24 to E&M services provided during post-operative periods. On these types of encounters, the system should have a hard stop that will prevent this claim from automatically being billed, so it can be reviewed to see if billing for the service is appropriate.

Third, trends identified through audit and claims submission should be tracked. Reports of trend information should be established, at a minimum, on a monthly basis to help analyze findings of trends in noncompliant practices that can place the organization at risk. This information is crucial when providing feedback to providers and will help your Compliance department identify outliers.

Lastly, a critical step is educating your providers and billing staff on your findings. Make sure they know what items are included in global procedures. Continuous education will help empower your providers and staff and will help mitigate compliance risks in the future. Education should be provided frequently throughout the year, to keep the information fresh in everyone's minds. This education is key in helping providers and staff understand how crucial their role is and that what they report can and will impact not only them, but the entire organization. ■

1 CMS: Medicare Claims Processing Manual. Publication #100-04, chapter 12, section 40. Available at https://www.cms.gov/manuals/iom/list.asp
2 OIG FY 2010 Work Plan is available at http://oig.hhs.gov/publications/docs/workplan/2010/Work_Plan_FY_2010.pdf

Achieving "meaningful use" compliance in the Medicare FFS incentive program

By Janice A. Anderson, JD, BSN and Rebecca L. Frigy, JD, MPH

Editor's note: Janice A. Anderson, Shareholder in the Chicago offices of Polsinelli Shughart PC, has over 25 years' experience focusing on health regulatory and compliance issues and over 30 years' experience working in the health care industry. She may be contacted by e-mail at janderson@polisnelli.com or by telephone at 312/873-3623.

Rebecca L. Frigy is an attorney in the St. Louis offices of Polsinelli Shughart PC. She may be contacted by e-mail at rfrigy@polsinelli.com or by telephone at 314/889-7013.

The American Recovery and Reinvestment Act (ARRA), passed in February of 2009 with the Health Information Technology for Economic and Clinical Health Act (HITECH), established several incentive programs focused on promoting the adoption of electronic health record (EHR) technology: a Medicare Fee-For-Service (FFS) incentive program, a Medicare Advantage (MA) incentive program, and a Medicaid incentive program. (A discussion of the MA and Medicaid incentive programs will be included in future issues.) Although the three programs are separate and distinct, they have many common elements, particularly related to demonstrating and achieving meaningful use. Through these incentive programs, the government anticipates it will make over $20 billion in incentives available to providers who "meaningfully use" certified EHR technology. The incentive programs conceptualized by HITECH will be implemented through several rounds of rulemaking by the Centers for Medicare and Medicaid Services (CMS). The regulations promulgated so far, and those that will be promulgated in the future, set forth the standards that a provider must meet to achieve "meaningful use," the details regarding how incentive payments will be calculated and made, and certain certification criteria that the EHRs used by providers must meet. The Office of the National Coordinator for Health Information Technology (ONCHIT) is the government body charged with establishing the certification criteria for EHRs and health information technology (HIT). Providers must use EHRs that meet such certification criteria to achieve meaningful use; however, merely meeting the certification criteria alone is not enough to qualify as a meaningful user of EHR technology.

Two sets of final regulations related to meaningful use were simultaneously released on July 13, 2010 by CMS and by ONCHIT. The Final Rule from CMS sets forth the criteria required to achieve meaningful use by eligible professionals (EPs), eligible hospitals (EHs), and critical access hospitals (CAHs) in the first stage of the incentive programs; the relevant time lines for each incentive program; and the amount of incentive payments that a provider may be eligible for in each program. The details related to the Medicare Fee for Service (FFS) incentive program and a discussion of potential legal pitfalls of the incentive programs are summarized in this article.

The Final Rule creates incentives under the Medicare FFS program (as well as MA and Medicaid programs) for EPs, EHs, and CAHs to adopt and demonstrate meaningful use of certified EHR technology starting in 2011. The first payment year for EPs is any calendar year (CY) beginning with CY 2011; and for EHs and CAHs, it is any fiscal year (FY) beginning in federal FY 2011, which began October 1, 2010. This means that EHs and CAHs may begin qualifying for incentives for payment year 2011 as early as October 1, 2010. Although it is not clear in the regulations, it appears that this does not mean that EHs and CAHs must qualify for incentive payments on October 1, 2010, but rather must qualify for the incentive payments (by meeting all of the meaningful use requirements for a period of 90 days) during federal fiscal year 2011. The Final Rule also includes payment adjustments (penalties) under the Medicare FFS and MA programs for EPs, EHs, and CAHs that fail to adopt and demonstrate meaningful use after 2015.

Medicare incentive payments to eligible professionals

Medicare EPs who may qualify for the incentive by demonstrating meaningful use are doctors of medicine or osteopathy, doctors of dental surgery or dental medicine, doctors of podiatric medicine, doctors of optometry, or chiropractors who are legally authorized to practice under state law. Under The Final Rule, hospital-based EPs are not eligible to

receive the Medicare incentive payments. By definition, hospital-based EPs furnish 90% or more of their allowed services in hospital inpatient or emergency department settings, including all settings that meet the definition of the main provider, department of a provider, or having a provider-based status.

Under the Medicare FFS incentive program:

- Qualifying EPs are entitled to receive incentives for up to five years, with payments beginning as early as CY 2011.
- No incentives will be paid after CY 2016.
- Incentive payments will be equal to 75% of the Medicare allowable charges for covered professional services furnished by the EP in a payment year, subject to the incentive payment maximums.
- The aggregate maximum amount of total incentive payments that an EP can receive under the Medicare FFS incentive program is $44,000.
- If the EP "predominantly furnishes" professional services (i.e., more than 50%) in a Health Professional Shortage Area (HPSA), the maximum annual incentive amounts are increased by 10%.
- EPs who become meaningful users after CY 2014 will not be eligible to receive incentive payments.

Table 1 shows the maximum incentive payment amounts available each year to EPs in a non-HPSA under the Medicare FFS incentive program.

Table 1

Meaningful Use Established	EP Medicare Incentive Payment						
	2011	2012	2013	2014	2015	2016	Total
2011	$18,000	$12,000	$8,000	$4,000	$2,000	0	$44,000
2012		$18,000	$12,000	$8,000	$4,000	$2,000	$44,000
2013			$18,000	$12,000	$8,000	$4,000	$39,000
2014				$12,000	$8,000	$4,000	$24,000
2015					0	0	0

Beginning in CY 2015, if an EP has not established meaningful use, the Medicare physician fee schedule amount for covered professional services furnished by the EP during the year will be reduced by applying a sliding scale percentage reduction to the fee schedule amount that would otherwise apply. For 2015, an EP who does not meet the meaningful use requirements would receive:

- only 99% of the Medicare fee schedule amount (or if the EP is also not a successful e-prescriber, 98%),
- only 98% for 2016, and
- only 97% for 2017 and beyond.

Under the Medicare Improvements for Patients and Providers Act (MIPPA), with respect to covered professional services furnished by an EP during 2012 or any subsequent year, if the EP is not a successful e-prescriber for the year, the fee schedule amount for such services will be reduced by 1% for 2012; 1.5% for 2013; and 2% for 2014 and each subsequent year. The HITECH Act and The Final Rule do not have any effect on MIPPA; and therefore, these reductions will begin in 2012 as legislated. However, neither MIPPA, nor the HITECH Act and The Final Rule provide that there will be a reduction in the reimbursement amounts that the EP would otherwise have been entitled to receive. Therefore, CY 2015 is the only year in which an EP would face an additional 1% decrease if such EP was not a successful e-prescriber, because in subsequent years, the meaningful use reductions would be equal to or greater than a 2% fee reduction.

Incentive payments under the Medicare FFS incentive program will be made to qualifying EPs in a single, consolidated annual payment through Medicare Administrative Contractors (MAC) or Carriers. Incentive payments will be made on a rolling basis as soon as the MAC ascertains that an EP successfully demonstrated meaningful use for the applicable reporting period (that is, 90 days for the first year and a full calendar year for subsequent years). The incentive payments will be made to the Tax Identification Number (TIN) provided by the EP. For EPs associated with more than one practice, CMS requires that the EP select only one TIN to receive applicable EHR incentive payments. EPs are allowed to reassign incentive payments to an employer or an entity with which they have a valid employment agreement or contract providing for such reassignment.

Unlike EHs, which may participate in both the Medicare FFS and the Medicaid incentive programs, EPs may participate in only one program. CMS has proposed to allow each EP to designate its program of choice and to allow the EP to change its designation one time before 2014.

Incentive payments to eligible hospitals

An EH is a hospital paid under the hospital Inpatient Prospective Payment System (IPPS) that is located in one of the 50 states or the District of Columbia. Eligible hospitals do not include psychiatric, rehabilitation, long-term care, children's hospitals, or cancer hospitals, which are excluded from the IPPS. Qualifying CAHs include all certified critical access hospitals.

Under the Medicare FFS incentive program:

- A qualifying EH or CAH may receive incentive payments for up to four years, beginning FY 2011.
- FY 2015 is the last year for which an EH or CAH can begin receiving incentive payments for meaningful use.

Continued on page 32

 ...continued from page 31

- An EH or CAH can qualify to receive payments from both the Medicare and Medicaid EHR incentive programs.
- Incentive payments for EHs and CAHs are calculated based on the provider number used for cost reporting purposes, which is the CMS Certification Number (CCN) of the main provider (also referred to as OSCAR number).

In determining incentive payment amounts, the EH's incentive payment will be based on the hospital's Medicare Part A and MA inpatient bed days, total inpatient bed days, and charges for charity care. In contrast, CAHs can receive incentive payments for the reasonable costs incurred for the purchase of depreciable assets such as computers, hardware, and software necessary to administer certified EHR technology, excluding all depreciation and interest expenses associated with acquisition. The incentive payments received by a CAH will be equal to the product of the CAH's reasonable costs incurred for the purchase of certified EHR technology and its Medicare share percentage. (The Medicare share percentage of a CAH equals the lesser of (1) 100%; or (2) the sum of the Medicare share fraction for the CAH and 20 percentage points.)

CMS will determine incentive payments at the time of settling the 12-month Cost Report for the EH's fiscal year after the beginning of the payment year. The data used will be based on the hospital discharge and other data from that Cost Report period, once the hospital has qualified for meaningful use. Fiscal Intermediaries (FIs) and MACs will calculate incentive payments for qualifying EHs and CAHs, and will disburse such payments on an interim basis, once the EH or CAH has demonstrated meaningful use for the EHR reporting period.

Like EPs, EHs and CAHs that do not meet the meaningful use requirements by FY 2015 and beyond will be subject to penalties in the form of reductions in reimbursement. EHs that do not meet the meaningful use requirements will incur 25%, 50%, and 75% reductions of their market basket updates in FY 2015, FY 2016, and FY 2017 and subsequent years, respectively. CAH reimbursement for those CAHs that fail to meet the meaningful use requirements by 2015 will be reduced from 101% of its reasonable costs to 100.66%, 100.33%, and 100% in the cost reporting periods beginning in FY 2015, 2016, and 2017 and beyond, respectively.

CMS will also conduct selected compliance reviews of EPs, EHs, and qualified CAHs that register for the incentive programs and are recipients of incentive payments for the meaningful use of certified EHR technology.

- uses certified EHR technology to submit information to the Secretary of CMS on specified clinical quality measures and other measures.

The meaningful use criteria will be rolled out by CMS in three "stages" and it is anticipated that each of the stages will build on the criteria in the prior stage. The Final Rule includes the criteria for Stage 1 only, and CMS has not yet proposed criteria for Stages 2 and 3. CMS expects to update the meaningful use criteria on a biennial basis, with the Stage 2 criteria being released by the end of 2011 and the Stage 3 criteria being released by the end of 2013. Depending on the payment year in which an EP, EH, or CAH establishes meaningful use, the provider will have to meet the relevant criteria. Table 2 outlines how CMS anticipates applying the stages of meaningful use criteria in the first years of the program.

Table 2

First Payment Year	Criteria Required by Payment Year				
	2011	2012	2013	2014	2015
2011	Stage 1	Stage 1	Stage 2	Stage 2	TBD
2012		Stage 1	Stage 1	Stage 2	TBD
2013			Stage 1	Stage 1	TBD
2014				Stage 1	TBD

Criteria and incentive timeline for achieving meaningful use

An EP or EH is considered a "meaningful user" of EHR technology and will receive the incentive payments described above, if, during the specified reporting period, it:

- demonstrates use of certified EHR technology in a meaningful manner;
- demonstrates that the certified EHR technology is connected in a manner that provides for the electronic exchange of health information in order to improve the quality of health care, such as promoting care coordination; and

Under the Final Rule, EPs, EHs, and CAHs seeking to achieve Stage 1 meaningful use must be able to meet 14 required criteria objectives for EHs/CAHs and 15 required criteria objectives for EPs, and 5 of 10 optional criteria objectives with their associated measures which are found on a "menu" of 10 optional criteria objectives. The required criteria objectives that an EP, EH, or CAH must meet include:

- Use computerized prescriber order entry (CPOE) for medication orders directly entered by any licensed health care professional;

- Implement drug-drug and drug-allergy interaction checks;
- Generate and transmit permissible prescriptions electronically (EPs only);
- Record certain demographics, including gender, preferred language, race, ethnicity, date of birth, and date and preliminary cause of death in the event of mortality in the EH or CAH;
- Maintain an up-to-date problem list of current and active diagnoses;
- Maintain an active medication list;
- Maintain an active medication allergy list;
- Record and chart changes in vital signs including height, weight, and blood pressure; calculate and display BMI; and plot and display growth charts including BMI for patients 2–20 years old;
- Record smoking status for patients age 13 years or older;
- Implement one clinical decision support rule related to a high priority condition with the ability to track compliance with that rule;
- Report quality measures to CMS or the states;
- Provide patients with an electronic copy of their health information, including diagnostic test results, a problem list, medication lists, medication allergies, and discharge summaries and procedures upon request (EHs/CAHs only);
- Provide patients with an electronic copy of their discharge instructions at time of discharge, upon request (EHs/CAHs only);
- Provide clinical summaries for patients for each office visit;
- Able to exchange key clinical information among providers of care and patient-authorized entities electronically; and
- Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.

EPs/EHs/CAHs also must meet five of the menu set of criteria objectives, including:

- Implement drug-formulary checks;
- Record advanced directives for patients age 65 years or older (EHs/CAHs only);
- Incorporate clinical lab test results into certified EHR technology as structured data;
- Generate lists of patients by specific conditions to use for quality improvement, reduction of disparities, and research or outreach;
- Send reminders to patients per patient preference for preventive/follow-up care (EPs only);
- Provide patients with timely electronic access to their health information within four business days of the information being available to the EP (EPs only);
- Use certified EHR technology to identify patient-specific education resources and provide those resources to the patient, if appropriate;
- Perform medication reconciliation upon receiving a patient from another setting or provider of care;
- Provide a summary-of-care record for each transition of care or referral if transitioning or referring a patient to another setting or provider of care;
- Able to submit electronic data to immunization registries or immunization information systems and actual submissions in accordance with applicable law and practice;
- Able to report electronic data on reportable lab results to public health agencies (as required by state or local law) and make actual submission in accordance with applicable law and practice (EHs/CAHs only); and
- Able to submit electronic syndromic surveillance data to public health agencies and make actual submission in accordance with applicable law and practice. (Note: The criteria right now is the ability to make these submissions – there are questions related to whether or not the immunization registries and public health agencies all have the ability to receive this type of data electronically right now, and the EP/EH/CAH should not be penalized.)

One of the requirements that must be met in order to achieve "meaningful use" is that the EP, EH, or CAH must use certified EHR technology to submit information to the Secretary of CMS on specified clinical quality measures and other measures. Under The Final Rule, EPs are required to report data on three core quality measures in CY 2011 and 2012: blood-pressure level, tobacco use status, and adult weight screening and follow-up. Some alternate quality measures (to which the above quality measures do not apply) are: weight assessment and counseling for children, influenza immunization, and childhood immunization status.

Notably, to meet the meaningful use requirements, EPs need only report the required clinical quality measures; they need not satisfy a minimum value for any of the clinical quality measures. Additionally, EPs must also choose three other measures (from a list of 38) that it is able to incorporate into its EHRs. Similarly, by payment year 2011-2012, EHs and CAHs will be required to report on each of 15 clinical quality measures that are included in the Reporting Hospital Quality Data for Annual Payment Update (RHQDAPU). Again, for EHs and CAHs, the report must only be made and a minimum value need not be satisfied. The 15 RHQDAPU measures are:

- Admitted patients' median time from emergency department (ED) arrival to ED departure;
- Admission decision time to ED departure time for admitted patients;

Continued on page 34

Achieving "meaningful use" compliance in the Medicare FFS incentive program *...continued from page 33*

- Ischemic stroke patients prescribed antithrombotic therapy at hospital discharge;
- Ischemic stroke – anticoagulation for atrial-fib/flutter;
- Ischemic stroke – thrombolytic therapy for patients arriving within 2 hours of symptom onset;
- Ischemic or hemorrhagic stroke – antithrombotic therapy by Day 2;
- Ischemic stroke – discharge on statins;
- Ischemic or hemorrhagic stroke – stroke education;
- Ischemic or hemorrhagic stroke – rehabilitation assessment;
- Venous thrombo embolism (VTE) prophylaxis within 24 hours of arrival;
- Intensive Care Unit VTE prophylaxis;
- VTE anticoagulation overlap therapy;
- VTE platelet monitoring on unfractionated heparin;
- VTE discharge instructions; and
- Incidence of potentially preventable VTE.

To receive incentive payments in payment year 2011, a provider may use an attestation method to submit summary information to CMS relating to each quality measure, rather than submitting such information electronically. However, starting in payment year 2012, in addition to meeting requirements for meaningful use, Medicare EPs, EHs, and CAHs will be required to electronically submit clinical quality measure results (numerators, denominators, exclusions) as calculated by certified EHR technology.

In the first payment year only, a provider need only satisfy the Stage 1 criteria for any continuous 90-day period during the payment year in order to qualify for an incentive payment. After the initial payment year, however, the provider must meet all of the Stage 1 criteria for the entire payment year. This gives providers some leeway in getting EHR technology up and running in FY 2010. However, providers should consider attempting to meet more than the minimum Stage 1 meaningful use criteria from the outset, as CMS has indicated that all Stage 1 criteria objectives, including all "menu" set objectives, will likely be a required in later stages.

Use of certified EHR technology

As described above, in order to achieve meaningful use of EHRs, a provider must use certified EHR technology. In conjunction with the release of The Final Rule, ONCHIT released the Certification Criteria Final Rule, which details the standards, implementation specifications, and certification criteria for EHR technology required for Stage 1 of the incentive programs (Certification Criteria).

The Certification Criteria represent the floor of the EHR technology's capabilities required for the incentive programs; the minimum requirements that EHR technology must meet in order to achieve certification. It is not, however, intended to act as a limit on the use of additional functionality or capabilities of EHR technology generally.

Additionally, it is important to note that the Certification Criteria Final Rule is not intended to specify the conditions under which adopted Certification Criteria must be used. Instead, it specifies the minimum functionality an EHR must demonstrate to attain certification. Certifiable EHR technology need only be capable of demonstrating the ability to comply with the Certification Criteria.

ONCHIT contemplates an evolving list of standards for continued certification going forward. Alterations and updates for subsequent stages (Stages 2 and 3) will be released on a biennial basis with intermediate "Optional Criteria" in the years between (which are expected to foreshadow coming changes in each biennial release). On the horizon, then, will be a series of optional criteria needed for certification preceding each new mandatory stage. This phased-in approach is designed to provide a vehicle for ongoing dialog with ONCHIT and providers, vendors, and the health care community-at-large on the topic of the meaningful use of Certified EHR Technology.

Potential legal pitfalls

As discussed above, it is estimated that CMS will make more than $20 billion in incentive payments to providers that meaningfully use certified EHR technology. Generally, where so much money is available from the government for a specified legitimate purpose, the stage is also set for individuals to inappropriately and fraudulently take advantage of the incentive programs. The three EHR meaningful use incentive programs will likely be no different than any other government program, and fraud is just one of several potential legal pitfalls.

Due to the expected large number of applicants for EHR incentives under the three incentive programs, it seems unlikely that CMS will be able to verify every applicant's assertion of meaningful use compliance. CMS may utilize its existing systems, such as the Provider Enrollment, Chain and Ownership System (PECOS) and National Plan and Provider Enumeration System (NPPES), to verify that applicants fall within a group that is eligible for the incentives in the first place; however, there are no corresponding mechanisms to check whether a provider has achieved compliance with the minimum necessary meaningful use measures. CMS will likely rely on random compliance audits and other verification methods of sampling applicants' compliance with the meaningful use criteria, such as expanding the Recover Audit Contractor (RAC) audits to include meaningful use compliance. This approach leaves it up to each applicant organization to hold itself to the appropriate level of internal oversight when determining compliance, and it is likely that a failure to do so could result in liability and penalties under the False Claims Act.

Additionally, one of the requirements to achieve meaningful use is for the provider to report certain clinical quality indicators to CMS. The Final Rule, however, does not require that a provider meet a minimum level of clinical quality measures. Nonetheless, the use of such clinical quality indicators by CMS to determine whether medical services were appropriately rendered is likely not far off, as CMS will implement Value Based Purchasing in FY 2013.[1] This quality reporting requirement may result in allegations of False Claims Act liability if the quality metrics are not accurate, the services are not rendered, or possibly even if the services rendered are below the standard of care.

Finally, the incentive programs should act as a motivating factor for providers to invest in and adopt the use of EHR technology, particularly given the reduction in Medicare fee schedule payments to providers who do not meet the meaningful use criteria by 2015. Because of this, many EPs will search for sources of funding to help adopt the use of EHR technology. One source of this funding may be the donation of EHR technology by hospitals with which the EP is affiliated. This practice is acceptable under both the Anti-kickback Statute and the Stark Law as long as each donation fits within the applicable EHR donation safe harbor and exception, respectively. Prior to a hospital donating EHR technology to an EP, however, legal counsel should review and approve the arrangement to help ensure that the donation meets all of the requirements of the applicable safe harbor and exception. ■

1 Patient Protection and Affordability Care Act § 3001.

Tankersley named Shareholder

HCCA member Regan E. Tankersley has recently been named a Shareholder at Hall, Render, Killian, Heath & Lyman, a national health law firm with offices in Indiana, Kentucky, Michigan and Wisconsin.

Dos and don'ts of policy writing

By Nicola Heslip, RN, BSN, CPHQ, LNC, CPSO

Editor's note: Nicola Heslip is a Certified Professional in Healthcare Quality at PolicyMedical™. Nicola has over twenty years of experience in the health care industry as a Registered Nurse, Certified Legal Nurse Consultant, and Certified Professional in Healthcare Quality, among other roles. She may be contacted by e-mail at nicola@policymedical.com or by telephone at 253/217-7180.

Patient safety is truly the foundation of any health care organization. It is a way of thinking; a way of acting. Really, it's a vision to do no patient harm. When we think about how documents (such as policies and procedures) guide patient care, our thought process is that by following them, there will be a positive outcome (i.e., patient safety). But in truth, excellent care given is a reflection of a well-written policy or procedure.

Health care policies and procedures are molded and shaped by many factors. One is health care regulations, such as state and federal mandates. Another is evidence-based practices, as we have seen with the patient safety movement. Lastly, there are accreditation standards that impact the content of policies and procedures, such as those set by The Joint Commission. Creating these documents is an art and with any form of art, we know that the expertise doesn't develop overnight. That being said, here are some key points to consider when creating the tapestries that guide our health care providers.

Finding a thought expert

Policies and procedures should not be written by those who are not experts on the topic. Consider the organization that asks its compliance officer to single-handedly write policies related to informed consent. Yes, there are some compliance officers who have a background in health care law, who know about consent and what is required by the state or CMS. For example, they'll know that only a licensed provider can obtain informed consent. But, do they know:

- What is the current process in the organization?
- How does the informed consent form get to the physician for use during the process of obtaining consent from the patient?
- How does the copy find its way into the patient's chart, if consent is obtained in the doctor's office?
- When can the nurse witness the consent?
- How are the needs of non-English speaking patients met during the consent process?
- Can the interpreter witness the consent?
- What auditing is done to ensure that the forms are being completed per CMS guidelines?

All of these elements—and more—need to be incorporated into the policies and procedures for health care staff to reference. Is the officer who writes your policies equipped to answer these questions?

One size does not fit all

Policies and procedures should not be written under the assumption that one size fits all. For example, a hospital may have read the requirements for The Joint Commission's National Patient Safety Goal on Hand Off, and they may have decided that SBAR (Situation Background Assessment and Recommendations), a model that is evidenced-based and commonly used for physician-nurse communication, is the right one to cite in the general policy related to hand off in that hospital. However, an area of the hospital may be using a different tool that meets the intent of this safety goal, and precautions need to be taken to make sure that all other policies on hand off should cross-reference this department-specific policy.

Too often, a policy committee will sit down anxiously and begin work on a new policy, without first identifying any existing policies on that topic. If there is an ambulatory center or primary clinic under the hospital's license, those areas are considered another "department" and the hospital policy committee needs to ensure that those departments' policies are reviewed as well. A big mistake is to make a generic house-wide policy on hand off that ignores what is being done elsewhere. During any survey performed by an outside auditor, the surveyor will surely visit those other areas and find a completely different policy on hand off. This is when you'll get caught for your lack of oversight. But, as long as the generic policy acknowledges or reference the department-specific policy and there is some way to link them, you then avoid those "silos."

Originality is underrated

A common problem in the world of policies and procedures is the existence of a document that is just a copy-and-paste of the literature source. Policies and procedures should not be merely a page torn out from a textbook! Yet, too often, I see clinics that have guidelines from the same reference book that just lists all the policies and procedures in order, based on the patient's condition. In practice, if the patient calls with stomach pains, the nurse looks at the guideline that states "See pg 125

of reference X" and then searches page 125 to see the protocol to follow for that patient. The nurse would then document in the triage record that he/she used Reference X per protocol and page 125.

There have been policies that mimic the content from The Joint Commission's Comprehensive Accreditation Manual for Hospitals (CAMH) word for word. Having language from regulatory texts is not the problem; it shows the surveyor who reads the document that the organization is aware of the requirement. The difficulty, however, is when the copy-and-paste text includes so much irrelevant information that it discourages the staff from reading the policy in the first place. It gives the staff incentive to sign off on it without reading it thoroughly. Even worse, there are times when staff has been instructed to carry out a procedure in a way that is standardized to that hospital, but the copy-and-pasted material describes a completely different method. When the surveyor comes, staff is asked about the policy and they state something different from the actual policy.

It is useless to simply ensure that the policies and procedures in your hospital reflect the requirements stated in reference books, if they're not written in a way that's easy for your frontline staff to interpret and apply. In between surveys, hospitals complete The Joint Commission Periodic Performance Review (PPR), which is a self assessment of how they are meeting the standards. Sadly, it is a disservice to the hospital if they score themselves compliant because the policy contains the wording of the requirement, but that is not actually how the procedure is done in that organization.

Standardized formats

Time management is a key issue for all staff who care for patients. Having the policy or procedure easily accessible is great, but can the staff easily find the information that they are looking for within the document? Policies and procedures should be written using a standardized writing format or style, so that staff members looking up any policy will know what section they need to go to for the right information. The organization needs to choose a format and stick with it.

There are experts in this field, like Stephen B. Page, who have excellent resources for writing policies and procedures.[1] His format consists of eight parts: Purpose, Persons Affected, Policy, Definitions, Responsibilities, Procedures, Document Approvals, and Change History. His books explain what content goes in each of these sections. Having all the policies and procedures in a standardized format also makes them easier to revise. For example, if The Joint Commission changes their standard on hand off, and it means a change in nursing practice, that information would be added to the procedure section of the document. The individual revising it could just go to that section, versus reading through the entire document and plugging in the new content. Often, there is a lot of narrative text in a procedure that doesn't flow well, and someone may have to fumble with where they are supposed to insert the new or revised information. Adding words to a document that guides patient care should not be not a crap shoot.

Finding the right policy reviewer

Policies and procedures need to be reviewed by a regulatory expert, and preferably someone who has experience in patient safety. Someone who can also filter for risk/legal issues would also be of benefit. The person(s) writing policies should have the experience and the skills to facilitate policy development, which means ensuring that all the right people review the documents. In addition, this person could wear several hats, such as clinical risk management, regulatory compliance, and patient safety. By wearing these hats, this person will be able to map out work flow processes and perform gap analyses based on the requirements. They can read the policy or procedure and determine what is not currently being done by staff and what should be tweaked to make the actual process match the document. If a requirement dictates a complete change in how care is delivered, then that will mean communicating the behavior change to the educators for implementation. A likely place to find this individual is in the Quality department.

Frontline staff involvement

A critical component of policy and procedure writing is frontline staff involvement. This can be accomplished by having a consultant and/or a standing member of a policy and procedure committee involved during the initial phase of policy and procedure development and the pilot/pre-rollout phase of implementation. The bedside caregiver uses the policies and procedures and knows best in terms of what is current practice. A group of leaders and compliance staff can meet and come up with an "ideal" process, but they need to find out what is really happening on the floor. Involving staff can help avoid the hassle of re-working policies and procedures that were written based on assumptions.

The frontline staff also are more prone to buying-in to the change that comes from a new policy or procedure if they were allowed to provide feedback and insight in the beginning. After all, it impacts their work flow. We should work with them to intermix what has to be done with how we can best make it happen.

Often the nay-sayers appear whenever there is a change in practice, because they feel overlooked in the whole decision-making process. To them, it appears that without warning, they

Continued on page 38

 ...continued from page 37

come to work one day and find that the policy and procedure they use regularly has been changed. They are told, "It has to be done this way." They see it coming from "higher ups," and if the change is not realistic or it doesn't appear that "x, y, z" have been considered, then there will be considerable push back from the nursing staff. These are the situations in which we find that nurses are not "compliant" with carrying out the practices stipulated in the policies, or are not documenting in the records as expected. Later we find out that the policy was rolled out without communicating the impact on the charting piece or the forms. Nurses need to be involved to make this a win-win situation.

Conclusion

Many organizations feel they are "compliant" with regulatory requirements, because they have a policy or procedure that is appropriately titled after the name of the pertinent regulation or standard. Having a policy or procedure titled Hand Hygiene is a starting point, yes—but has the content been written by an Infection Control practitioner, someone who is an expert on the subject and who has been on the floors rounding for infection control surveillance? Is the policy written to cover the hospital as well as outpatient areas? Does it ensure that the content is specific and relevant to those settings? Remember: one size doesn't fit them all. Is the policy content a word-for-word version of **Mosby's Textbook for Nursing Assistants**, or does it incorporate how the process is actually practiced in the facility? Is the policy in a standardized format so that staff can quickly scroll through it to find the information they need?

Has the Hand Hygiene policy, for example, been looked over by a patient safety expert who has that regulatory/legal eye? After all, this person is key to interpreting the standards. The patient safety expert can decipher what the standard is really going for, and make sure that, for example, we don't make our policies and procedures more stringent than necessary. And at the end of the day, they can translate what the policy stipulates (what needs to happen) into a realistic process. This individual knows the organization from doing safety rounds on the units and has a close relationship with the staff.

Lastly, look into whether the policy or procedure has been tested on the staff. The patient outcome is determined by how nurses carry out what those documents state. Engagement and trust are key to a successful rollout. Let staff be part of decision-making when it comes to practice. Bring them on board. You are sure to move into a culture of policies and procedures that makes compliance and getting ready for the next survey as natural as getting ready for the next patient. ■

1 Stephen B. Page: *Establishing a System of Policies and Procedures.* Process Improvement Publisher; 7th Revision edition (1998) and *Best Practices in Policies and Procedures.* Process Improvement Publishing; 3rd edition (July 12, 2010)

Employment references: Name, rank, serial number... is that all there is?

By: Natalie Wyatt-Brown, Esq.

Editor's note: Natalie Wyatt-Brown is a Shareholder of Halleland Habicht and is the head of its Employment Department. She has been practicing law for 15 years, focusing on management-side employment law for the past 10 years. She has extensive experience dealing with various workplace issues, including providing training and counseling, responding to administrative charges, and litigation in state and federal courts. Ms. Brown may be contacted by telephone at 612/836-5500 or by e-mail at nwyatt-brown@hallelandhabicht.com.

As the person responsible for compliance, you may be asked for an employment reference, usually for a former employee. Although you probably have strong opinions about this employee, whether positive or negative, you know that you are only supposed to give out confirmation of dates of employment and, sometimes, last title held. But is that really all you can say? What about when the shoe is on the other foot? It would be nice to get more than just "name, rank, serial number" from a former employer when filling a position.

Is that all there is?

Most employers have resorted to the "name, rank, serial number" reference policy due to a fear of litigation. The primary concern is that an employer could be sued for defamation for giving a negative reference. Defamation is a false statement, tending to harm the reputation of the person in the community, which is published to a third party. Several defenses to a defamation claim may be used, however. A true statement, no matter how negative, cannot be defamatory as a matter of law. Similarly, a statement that is not as positive as the employee believes he or she deserves, but it not negative, is not defamatory. Further, a statement made for a proper purpose and upon a proper occasion is not actionable, unless the plaintiff can prove it was made with malice. This is referred to as the "qualified privilege," and it generally applies to employment references. Further, to be defamatory, the statement must be factual in nature; statements of opinion are not defamatory, because they cannot be proven true or false. What constitutes truth, opinion, and malice, however, are often questions of fact for a jury to decide, which makes defending such actions risky and expensive.

So, I'm just going to give positive references from now on.

In addition to a possible defamation claim based on a negative reference, employers also face a risk of suit based on a positive one. Employers who choose to give a reference may be liable for misrepresentation, if they provide incomplete or misleading information regarding a former employee.

What if I give neutral references for bad employees and positive references for good employees?

By treating different employees differently, employers run the risk of a discrimination or retaliation claim. An employee who receives either no reference or a limited reference, while other employees received more complete or informative references, may argue that the limited reference constitutes unfair treatment by the employer.

My state has a job reference immunity law. Doesn't that mean I am protected if I give a reference?

Currently, 37 states have passed laws that exempt employment references from defamation claims, in a clear effort to reduce these concerns and allow employers to provide more complete information. Typically, these statutes create a rebuttable presumption that an employer who provides a job reference acts in good faith. Some statutes accomplish a similar goal by conditioning the immunity on good faith without expressly offering a presumption of good faith. Under either formulation, plaintiffs cannot prevail in a defamation claim without proving that the reference provider did not act in good faith.

These statutes usually echo the language of common law defamation standards for abuse of the qualified privilege by providing that defendants forfeit the immunity when they knowingly provide false information, or act with reckless disregard for truth or falsity. A few states venture further, permitting plaintiffs to prove bad faith by demonstrating that the employer's reference violated nondiscrimination or civil rights laws, confidentiality, or other agreements.

The difficulty with most of these laws is the uncertainty surrounding what constitutes "good faith," which is often not defined, or is only defined in a vague or circular fashion. As a result, they often do not provide much further protection than the common law

Continued on page 40

qualified privilege for defamation claims. An employer may abuse the privilege by knowingly providing false information, by acting in reckless disregard for the truth or falsity of the information, by communicating the statements to persons who are not within the purpose of the privilege, or by excessive publication.

Maine's Employment Reference Immunity law[1] is a good example of the above. That statute provides:

> An employer who discloses information about a former employee's job performance or work record to a prospective employer is presumed to be acting in good faith and, unless lack of good faith is shown by clear and convincing evidence, is immune from civil liability for such disclosure or its consequences. Clear and convincing evidence of lack of good faith means evidence that clearly shows the knowing disclosure, with malicious intent, of false or deliberately misleading information. This section is supplemental to and not in derogation of any claims available to the former employee that exist under state law and any protections that are already afforded employers under state law.

Therefore, a Maine employer is immune from all civil liability for providing an employment reference absent "clear and convincing" evidence that the employer knew the information was false or misleading.

From Maine to California, Florida to Washington, and everywhere in between, most employers still refuse to provide detailed information regarding former employees. It is clear, therefore, that these statutes have not had their intended effect.

Do all states require "good faith"?

In an effort to get around the concerns described above, Minnesota passed a unique statute[2] on the subject. It is so different, in fact, that many articles and comments do not include it as one of the nation's job reference immunity laws. Unlike most states, Minnesota does not require the reference to be made in "good faith," but instead it depends on a complex series of very specific requirements before job reference immunity is conferred.

Subdivision 1 provides that an employee can ask an employer to remove disputed information from his or her personnel file. If the employer refuses, the employee may ask to submit a written position statement (not more than five pages long) that must be placed in the employee's personnel file.

Subdivision 2 of the statute provides that an employer is immune from a defamation claim for communicating information contained in an employee's personnel record, but only after the employee has reviewed his or her file. If the employee makes a request under Subdivision 1 and the employer agrees to remove or revise the disputed information or the employee submits a position statement, the employer is required to provide both the disputed information and the written position statement, or to follow its agreement with the employee to remove or revise it.

Therefore, if a Minnesota employer provides an employment reference to a prospective employer based on information contained in the former employee's personnel file, and the employee has reviewed and not disputed that information, the employer is totally immune from a suit for defamation without the messy fact issue of whether the employer acted in good faith. The problem is that most employees don't review their personnel files, even though they have the legal right to do so in Minnesota, which means the immunity almost never comes into play. Therefore, most Minnesota employers, like their colleagues across the nation, still follow the "name, rank, serial number" reference policy.

So why even bother getting references, if no one will say anything useful?

Even though most employers, even ones protected by reference immunity statutes, do not provide detailed references, there are reasons to continue to seek them.

First, employers should check references if only to confirm what applicants tell them. In one case, an employer did not bother to check references in the mistaken belief that he would not learn anything. After the employee had filed a fraudulent workers compensation claim and then a baseless charge of discrimination, a simple Internet search revealed that one of the prior employers listed on his job application did not even exist. Had the employer verified his prior employment, he would not have hired him, thus avoiding thousands of dollars in legal fees and other costs.

Getting around "Don't ask, don't tell"

Despite reluctance on the part of employers to give detailed references, there are ways for employers to gather useful information about prospective hires. The following is a list of tips and strategies to verify information, protect the company, and avoid liability.

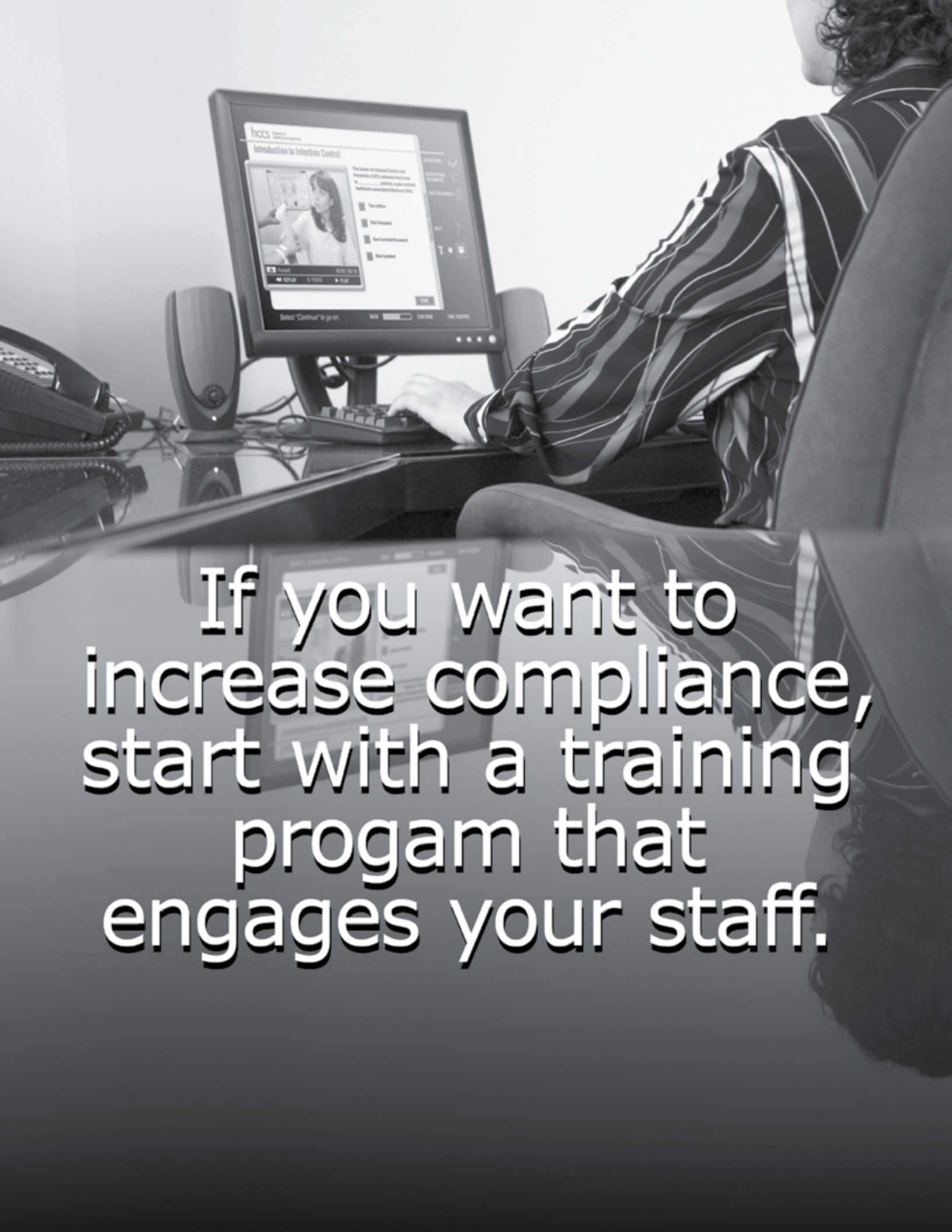
1. Ask applicants to explain specific periods of unemployment or gaps in their history, either on the application or during the interview.
2. Ask for all prior names used by the applicant.
3. Make clear to applicants in the interview that you will check their references.
4. During the interview, obtain names of several job-related references not listed on the application, and then contact those individuals.
5. Have applicants make necessary arrangements for you to talk with references you

choose. This puts the burden on applicants to ensure that these references are obtained.

6. Ask applicants to name former supervisors who should not be contacted for a reference and explain why.
7. Ask applicants to provide copies of past performance reviews.
8. Follow up on written references presented by the candidate.
9. Consider using a qualified outside firm to check references, especially for sensitive and upper-level positions.
10. Verify degrees and licenses listed on the application or resume.
11. Check references by phone or in person. The response rate to written requests is lower.
12. Check more than one reference.
13. Don't limit your reference contacts to those provided by the applicant.
14. If any employees in your organization are familiar with the applicant, ask for their opinions.
15. Develop a broad network of contacts to open up informal sources of reference checking.
16. Document every reference contacted, even if the individual contacted refused to provide reference information.
17. Try to avoid contacting the Human Resource department for references, unless there are no other contacts from the organization.
18. When making telephone reference checks, start with simple questions first.
19. Ask open-ended questions about employment history, job performance, and potential problems.
20. Never ask questions relating to age, race, sex, religion, national origin, marital status, disability, or any other protected status.
21. As appropriate for particular positions, check a prospective employee's criminal history, driving record, credit history, and Social Security number.
22. Evaluate negative references fairly. A negative response from one individual does not necessarily mean the candidate is unqualified or difficult to work with.
23. Keep reference documentation confidential.
24. Retain reference records for at least the minimum period required by law.

With these rules in mind, you should be able to gather useful information while at the same time avoiding liability. ■

1 Maine: Title 26 Labor and Industry, Chapter 7 Employment Law, Subchapter 1 Conditions for Employment, § 598 Employment Reference Immunity, 1995. Available at http://www.mainelegislature.org/legis/statutes/26/title26sec598.html.
2 Minnesota Statute § 181.962 (1990). Available at https://www.revisor.mn.gov/statutes/?id=181.962



If you want to increase compliance, start with a training progam that engages your staff.

Healthcare facilities that are serious about reducing risk choose HCCS.

Compliance is serious business and it takes a serious training program to increase awareness and change staff behavior. Compliance training must have emotional impact and must change attitudes to be effective.

Engaging, professionally designed multimedia content is more effective then page-turning text.

An effective training program requires more then asking your staff to flip through some electronic text pages. HCCS online compliance and competency training courseware uses professional multimedia elements to create an engaging, interactive learning environment. Real-life video scenarios with professional actors in healthcare settings, audio narration and interactivity are combined to increase the retention of the information presented.

Adult learning is what works.

HCCS courseware is designed using accepted principles of how adults learn and retain information.

Research shows that retention is greatest when the learner sees, hears and interacts with training content.

HCCS courses combine expert up-to-date content with expert learning methods to create a truly unique learning experience.

The top University hospitals in the country choose HCCS.

More than 50 Academic Medical Centers, 25 medical schools and hundreds of other healthcare facilities have chosen HCCS training courseware for their online education. With over one million registered learners, HCCS is the leading provider of online multimedia compliance and competency training courseware.

When employees pay attention, you reduce your risk.

Looking for a more effective training solution? Want to increase compliance?

Don't take our word for it, take one of our free educational webinars or test drive our courseware yourself at www.hccs.com.

hccs

Experts in Healthcare Learning

Call 877-933-4227 for more information and a schedule of **FREE training webinars** or go to www.hccs.com

Medicare • Medicaid • HIPAA • Quality Improvement • Research • Nursing

Protecting patient data is an all-inclusive deal

By K Royal

Editor's note: K Royal is the Privacy and Security Officer and Assistant Vice President, Regulatory Affairs for Concentra Inc. in Addison, Texas. She can be reached at 972/618-4714 or via email at K_Royal@concentra.com.

Health care entities function in a highly regulated environment. Not only are there federal laws that apply only to health care and related entities, but some state and federal laws apply simply as a cost of doing business in a technological world. Considering the realms in which health care entities operate (federal, state, and affiliated business standards), why would a physician want to expend the cost and effort to comply with even more guidelines? It appears to be the lament of many medical providers that they just want to treat patients, not deal with all the laws about data protection.

First, consider the types of data health care that entities collect in order to just treat patients. With one visit, a patient's file may contain full name, date of birth, age, sex, Social Security number, street address, city, state, zip code, phone number, e-mail, insurance, insurance ID number, employer, location, job title, names of family members, and much more—even before counting the actual medical information. This is everything a criminally minded individual would need in order to engage in some level of fraud.

Medical identity theft is a growing concern

Medical identity theft is either using another person's identity to obtain goods or services or as a money-making fraud scheme. The FBI reports cases of drug cartels/gangs abandoning the drug market in favor of medical fraud. For example, a fake medical clinic would bill for services provided to stolen medical identities. One such case was caught in Florida after having received over $100 million from Medicare. They had billed over $300 million.

Medical identity theft may result in insurance claims for items or services that have never been provided, were provided to an impersonator (with or without the true person's permission), or that are billed in exaggerated amounts. For the health care provider, these scenarios may result in unpaid claims, assessments of overpayments, or even accusations of fraudulent billing. For the individual whose identity is stolen, there are consequences beyond the obvious ones of credit collection attempts, and "maxing out" insurance benefits. Employment decisions are sometimes based on credit reports, as are any loans for homes, cars, or education. Having the medical information of two people combined also has a lingering impact. Even if the fraud is discovered and investigated, it could take a lifetime to sort out. Inaccuracies in medical records are sometimes difficult to correct and may never be entirely removed. With the new electronic health records (EHR), this particular problem can only grow, because it would be impossible to track every location where a piece of electronic data may reside. Certainly there are laws against fraud, but the burden of preventing crime has never fallen solely on those responsible for catching and prosecuting the criminals. If you park in downtown Chicago, don't leave the keys in the ignition.

Further, consider the concepts of negligence and standard of practice. If a car manufacturer made a door that did not lock and an ignition that started with anyone's touch, then the manufacturer would be negligent if the car was stolen. It is simply a standard practice in the automobile world that cars lock and a mechanism (usually a key) is required to start the car. This is a deterrent to petty criminals who may then look elsewhere for a free ride.

The health care world is similar in many respects. Both a standard of care for protecting patient data and potential negligence exist if the data is not protected correctly. Of course, this standard of practice for protecting patient data is not captured fully in one comprehensive regulatory framework; although the Health Insurance Portability and Accountability Act[1] (HIPAA) is certainly the most well-known and directly applicable. Other requirements that impact the protection of patient data include the Patient Identity Theft Protection Act, state laws, and Payment Card Industry Data Security Standards (PCI DSS) that apply to payments taken with credit cards.

HIPAA

As a federal law, HIPAA sets the floor for protecting patient data, but does not necessarily apply to all health care providers.[2] HIPAA applies to "covered entities" and their business associates (BAs). Covered entities are health care and related organizations, such as providers who make certain electronic transmissions, health care plans, and health care clearinghouses. Business associates perform actions and duties on behalf of the covered entity, and as of 2010, are accountable under HIPAA similar to covered entities. Examples of typical BAs are accounting firms, software vendors, medical record storage companies, or shredding companies. Thus, HIPAA applies to far more business than strictly health care.

HIPAA protects patient data through both the Privacy Rule and the Security Rule. The Privacy Rule dictates what information should be protected and how to use and disclose this protected information. The Security Rules provide how to actually protect the data.

Identity Theft Protection Act

The Federal Trade Commission (FTC) and several other federal agencies have mandated certain rules to prevent identity theft, called the Red Flags Rules under the Fair and Accurate Credit Transactions Act of 2003 (FACTA). Initially thought to apply only to financial institutions, it was established publicly that health care companies fall under the definition of "creditor." A creditor is defined as any person or business who arranges for the extension, renewal, or continuation of credit with a "covered account." A covered account is any account for personal, family, or household purposes. The FTC has made it very clear that if health care companies bill insurance, accept partial payments, and/or report to credit bureaus for collections (either directly or by using a service), then they must have a Red Flag program.

The Red Flag Rules must be written, approved by the board of directors, and must be appropriate to the size and complexity of organization and to the nature and scope of the business. The Rules must be under the direction of senior management, who are responsible for development, implementation, assessment.

However, it is unknown when, if ever, the Red Flag Rules will be enforced against health care providers. The American Medical Association (AMA), American Osteopathic Association (AOA), and the Medical Society of the District of Columbia have filed a lawsuit in federal court against the FTC for including physicians within the definition of "creditors" under its Identity Theft Protection Red Flag Rules. The physician groups state that HIPAA provides sufficient patient protection and that the requirement to set up an identity theft prevention and detection program is unnecessary. In their lawsuit, they argue that physicians do not qualify as "creditors" and that patients do not qualify as either "account holders" or "customers" under the Fair and Accurate Credit Transactions Act.

Originally, the Red Flag Rules were to take effect on Nov. 1, 2008, but there have been several delays: (1) May 1, 2009; (2) Aug. 1, 2009; (3) Nov. 1, 2009; and (4) June 1, 2010. They are currently scheduled to take effect December 31, 2010.

Understandably, the health care industry opposes more regulatory oversight; especially when so much of health care is self-regulated and governed by strict state standards. But when it comes to verifying patient identity, it doesn't make sense to fight it, when most providers are likely verifying patient identity anyway. It is sound business practice to verify that the customer in front of you is truly that person. Otherwise, no contract is valid, services are provided with no guarantee of reimbursement, Medicare fraud may be implicated, and depending on the medical history, there may even be malpractice. If the patient in front of you is not the patient represented on paper, then medical information gets co-mingled. In a small physician practice, this may not be a big concern; but in a pharmacy system or hospital, this could be life-threatening.

Treatments or medications may be prescribed based on incorrect medical information or history. Electronic Health Information Exchanges will further compound this concern.

The Red Flag Rules allow for a program that is suitable for the size, scope, and nature of the business. If the business is a one-physician office in a small town where the physician delivered his patients personally or has known them for decades, then the appropriate program can be miniscule in size. If the business is a multiple-hospital system across three states, then the program likely consists of some additions to the privacy and security program in place. Many of the necessary actions may already be present, such as checking a picture ID, updating addresses, and verifying insurance demographics.

Two groups of professionals have previously filed suit in the U.S. District Court of the District of Columbia against the FTC challenging Red Flags: attorneys[3] and Certified Public Accountants (CPAs). At this time, the attorneys, through the American Bar Association, have won on summary judgment and the FTC is appealing the case. For the CPAs, the District Court issued an order for the FTC to "continue to delay enforcement of the Red Flags Rule with respect to members of the AICPA [American Institute for CPAs] engaged in the practice of public accountancy for ninety (90) days after the U.S. Court of Appeals for the District of Columbia Circuit renders an opinion in the American Bar Association's case against the FTC."

The AMA and other professional groups have entered into an agreement with the FTC that the Red Flags Rule would not be enforced against health care providers until the ABA lawsuit is resolved on appeal. In addition, Currently, a bill (HR 3763/S3416) has passed the House and is making its way through the Senate. This bill specifically allows three professions: health care, accounting, and legal to be exempt from the Red Flag Rules, if they have 20 employees or less.

PCI DSS

The PCI DSS[4] is a set of global standards created to enhance account security, created

Continued on page 46

in part by most of the large credit card corporations including Discover, MasterCard, Visa, and American Express. PCI DSS was developed and is maintained to help businesses proactively protect relevant data. For health care providers, this is patient data. Essentially, if a provider accepts, stores, or transmits credit or debt cards as payment, then the PCI DSS apply. Keep in mind, in most cases, enforcement of PCI standards fall under the card brand, not a regulatory agency. However, three states have now incorporated PCI DSS into law: Minnesota, Nevada, and Washington.[5]

The extent of compliance action is dictated by the level of merchant activity. For example, a Level 4 merchant is one who processes less than 20,000 Visa e-commerce transactions annually, or up to $1 million regardless of format. In contrast, Level 1 merchants are those that process over six million Visa transactions annually, or a merchant that Visa determines should follow these standards in order to protect the Visa system. Yes, Visa dictates the levels.

PCI DSS compliance addresses twelve core requirements around secure networks, protecting data, managing vulnerabilities, controlling access, monitoring and testing networks, and maintaining security polices. Some of these requirements are also met if an organization is HIPAA compliant, such as controlling access to data on a need-to-know basis, protecting data, and maintaining security policies.

State laws

Currently, 45 states have enacted breach notification laws. Most breach notification laws apply to computer breaches, not paper breaches (as opposed to the federal breach laws which include hard copy or electronic data). In particular, Massachusetts and California appear to have the most proactive and extensive requirements around data security or medical information.

California Civil Code § 1798.82, et seq., provides that "any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, disclose any breach of the security system . . . to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." The law requires specific breach notification actions and applies whether the data is physically stored within the state or not. In 2008, California expanded the breach notification laws to specifically include medical and health information in the definition of "personal information." Thus, if this unencrypted information was obtained by an unauthorized person, the organization would be required to notify the individual. This law is not directed specifically towards health care providers; it applies to any business that maintains this information.

On the heels on California's breach laws, Massachusetts implemented the first laws that require protection of certain data, not just a response if that data is breached. This new law took effect in 2010, and requires businesses that license, store, or maintain personal information about a Massachusetts resident, to implement a comprehensive information security program that includes security policies, encryption, and monitoring of vulnerabilities. The solutions should be reasonable for the size, scope, and nature of the business. Like California, this applies to any residents of the state, not where the physical data resides.

Avoiding regulation

Health care providers that do not bill Medicare or Medicaid, do not electronically transmit data, do not take credit or debit cards for payment, and do not use computers can avoid most of the legal data protection requirements. The Red Flag Rules still require verification of patient identity. However, if all patients are required to pay in full up front – and no partial payments or deferred payments (such as billing insurance first) are allowed, then even the Red Flag Rules would not apply.

It is not feasible for the majority of health care providers to practice in a technologically- and regulatory-moot world. Realistically, providers collect data and a loss of that data or misrepresentation of that data due to identity issues can cause traumatic harm to the individuals whose data is collected. Mitigating that harm and withstanding the potential media storm could destroy a practice – or at least cause financial and ethical/malpractice concerns (many medical boards require appropriate confidentiality of records).

Conclusion

Extensive administrative burdens are not decreasing. However, health care is not the only targeted industry. Many reforms sweep across multiple business areas and some are industry-neutral. The emphasis is on protecting the patients and their data to the best of our ability. If the data is breached, the damages to your business can be devastating, including reputational damage. Patients expect their data to be protected. When that expectation coincides with sound business practice and regulatory oversight, it simply makes sense to take all reasonable steps to safeguard that data (and consider getting cyber-liability insurance coverage). In the technological environment in which health care functions, we will not see advances in medicine without also seeing advances in information security. ■

1 45 C.F.R. §§ 160 and 164.
2 This paper is not intended to review or analyze the full extent of HIPAA. Please see the U.S. Department of Health and Human Services, Office of Civil Rights website at http://www.hhs.gov/ocr/
3 American Bar Association vs. Federal Trade Commission, 671 F. Supp. 2d 64 (D.D.C. 2009). Also see American Bar Association, Governmental Affairs Office website at http://www.abanet.org/poladv/priorities/redflagrule/
4 For further information, please see PCI Compliance Guide website at http://www.pcicomplianceguide.org/
5 Minnesota Plastic Card Security Act, 2007; Nevada Security of Personal Information Law, 2009; and Washington State Bill 1149, 2010.

New HCCA Members

Alabama
- Mary Kathryn Crenshaw, Univ of Alabama
- Joseph L. Roberson, Univ of Alabama at Birmingham

Arizona
- Roseanne Berry, RBC Consulting, LLC
- Lindy A. Castillo, Arizona Counseling & Treatment Services
- Luciana Frank, Winslow Indian Health Care, Inc.
- Steven Guthrie, Pantano Behavioral Health Services, Inc.
- Andrew Harrington, The Guidance Center
- Rebekah Hays, The Guidance Center
- Brenda M. Hickernell, Southwest Behavioral Health Services
- Doug Jacobs, ABC Medical Billing Consultants
- Scott P. Leckey, Banner Estrella Medical Center
- Becky Salazar, St. Joseph's Hospital & Medical Center
- Vielka A. Velazquez, Magellan Health Services

Arkansas
- Darri L. Scalzo, Univ of Arkansas for Medical Sciences
- Michael Walker, Walmart Health & Wellness

California
- Therese Armstrong, Arista Labs
- Christos G. Arvanitis, Tenet Healthcare Doctors Hospital of Manteca
- Carlos J. Balladares, Dept of Public Health
- Chona G. Bautista-Peralta, City & County of San Francisco
- David Chook, Crescent Healthcare, Inc.
- Laura Churchill, AMN Healthcare
- Tara Cowell, Cowell Law Corporation
- Rick Dodds, Sonora Regional Medical Center
- Charmaine Dumont, Loma Linda UHS
- Edgar D. Escobedo, American Ambulance
- Timothy Felde, Care Ambulance Service
- Catherine Furtado, Kaiser Permanente
- Ronda Y. Gomez, El Centro Regional Medical Center
- Andrea Hammond, El Centro Regional Medical Center
- John Hansel, MedeAnalytics
- Latara Harris, Univ of California Berkeley
- Doug Hart, MedeAnalytics
- Jennifer E. Johnson, MedImpact Healthcare Systems, Inc
- Gary Kenney, GPK Consulting LLC
- Jennifer L. Kiff, United Indian Health Services Inc
- Greg Krantz, MedeAnalytics
- Whitney Laughlin, AMN Healthcare, Inc.
- Kristine F. LaVoy, Washington Hospital
- Leanne Link, Shasta County
- Robert Thomas Loughrey, St Joseph Health Syst
- Michele Marcotte, Molina Healthcare of California
- Jamie Marks, Children's Hospital Los Angeles
- Carol Ann Parker, Saint Louis Regional Hospital
- Charles Phelps, St Joseph Health System
- Emma Pickens, Kaiser Permanente
- Carissa Podesta, Ensign Facility Services
- Kristin Rand, Genentech
- Thaddeus San Pascual, Univ of California San Francisco
- Nate Seaman, MedeAnalytics
- Tina M. Sobotta, Marin General Hospital
- Matthew Soskins, Tri-City Medical Center
- Bonnie Vaughn, Diversified Clinical Services

Colorado
- Laurie Blumberg-Romero, The Children's Hospital
- Suzanne Brackley, ComplianceWorks LLC
- Bev Funaro, Yuma District Hospital & Clinics
- Brigitte Garner, Sinaiko Healthcare Consulting
- Carter Gilmer, Summit Compliance Services
- Saliha Greff, St Anthony North Hospital
- Kristen Lazare, Vail Valley Medical Center
- Constance McWilliams, Colorado Health Care Training and Consulting
- Le Meyer, Poudre Valley Health System
- Linda Michael, Centura Health
- Shari Shafer, Colorado West Healthcare System
- Jennifer E. Wilson, Colorado Hematology Oncology

Connecticut
- Patricia Bowen, UnitedHealth Group
- Lisa Frigo
- Gail Kinkead, Protiviti

Delaware
- Norene Broadhurst
- Mark M. DiDonato, Anesthesia Services, PA

Florida
- Lorna L. Betty, Blue Cross Blue Shield Florida
- Nancy Bongiovanni, Healthcare Strategies Group
- Sarah Crass, Hospital, Physician Partners
- Clarissa N. Glodis, South Florida Orthopaedics & Sports Medicine
- Eileen Horowitz, Hospital Physician Partners
- Gerald D. Jones, Pediatric Assoc of South Florida
- Troy A. Kishbaugh, GrayRobinson PA
- Terri MacFarlane, Lutheran Haven Inc
- Autumn Matthews, Matthews & Matthews, Attorneys at Law
- Scott Matthews, Matthews & Matthews, Attorneys at Law
- Karen Mulroe
- Carole Ramsay, Paradigm Health Services
- Michelle Riegler, Miami Behavioral Health Center
- Albert Saltiel, Pediatric Services of Florida
- Maricela Siller, Premier Community HealthCare Group Inc
- Rhonda G. White, Cornerstone Hospice

Georgia
- Luther Allison, Southern Regional Med Center
- Cynthia Badgio
- Lori Braatz, Gentiva
- Galen A Mirate, Mirate Eye Center
- Ben Overby, SBD Medical Solutions
- Monica Peete, Atlanta Medical Center
- Valerie Rock, GatesMoore
- Patrick Smith, North Atlanta Surgical Assoc
- Debra Sydnor, Alston & Bird LLP
- Debbie E. Thomas, Dorminy Medical Center

Hawaii
- Betty Eng, Clinical Laboratories of Hawaii, LLP
- August John Monge, Castle Medical Center
- Shawn Ripley, Kaiser Permanente

Illinois
- Joan Daniel, Advocate Healthcare
- Draco D. Forte, Sonnenschein
- Julie Grego, United Therapies
- Scott Jonkman, Walgreens
- Kelly A. Leach, Southern Illinois Univ-School of Medicine
- Lori A. Nelson, Family Service & Community Mental Health Center for McHenry County
- Marcie Ranick, Walgreens
- Caitlin J. Wilkes, Northwestern Univ

Indiana
- Daniel Carey, Otis R. Bowen Center
- Robert Greaney
- Nathan Kennedy, National Government Services
- Robert Stewart, The South Bend Clinic

Iowa
- Deborah Bradley, The Iowa Clinic
- Amy Piepmeier, Dallas County Hospital
- Michelle Swanstrom, ILA HLP

Kansas
- David Camp, Central Kansas Medical Center
- David C. Drovetta, Physicians Reference Laboratory
- Mindy Miller, Midwest Health Inc.

Kentucky
- Holly Brown
- Kathy Evans, Baptist Physicians Southeast
- Catherine I. Masoud, UK HealthCare
- Pat Olds, Pattie A. Clay Regional Med Center
- Amanda Padgett, Univ of Louisville

Compliance Today 2010 Index

Compliance 101

Durable Medical Equipment (DME)

Electronic Medical Records (EHR)

Feature Focus

Feature Interview

Continued on page 50

- What the small provider needs to know. June, p. 30; *T. Abell*
- Skilled nursing facility deficiencies: Provider rights and practical consideration. Sept, p. 42; *A.J. Markenson*

Medicare/Medicaid

- Adjudicating provider payment disputes: Medicare Advantage. Jan, p. 13; *S. Souers*
- RACs are coming to Medicare Advantage, Part D and Medicaid. Dec, p. 9; *G. Bryant*
- Medicare beneficiaries remain vulnerable to Medicare Advantage marketing schemes. Dec, p. *46; M. Stiglitz*

Pharmacy

- Feature Focus: Units reporting for drugs/biologicals: A growing area of compliance concern. April, p. 37; *M.G. Calahan*
- Integrating Pharmacy Operations and Compliance, Part 1. April. P. 31; *M.D. Vogelian*
- Integrating Pharmacy Operations and Compliance, Part 2: The 340B Program. June, p. 32; *M.D. Vogelian, J.L. Hobbs*
- E-prescribing of controlled substances: What do you have to do? Nov, p. 38; *L. Parking, S. Spinos*

Physician Practices

- Clarifying the confusing: The Anti-markup Rule made easy. Feb, p. 8; *T. Mantese, G. Nowakowski*
- Compliance 101: When the bill comes due: Insurance fraud and independent internal investigations. April, p. 44; *J.J. McGrath IV*
- Compliance programs: Critical for physician groups. April, p. 48; *B.A. Bredemeyer*
- The Stark Law and the "group practice" requirement. May, p. 44; *R. Ghafoorian*
- Mobility disabilities: A technical assistance manual for health care providers. Dec, p. 4; *D.H. Ganz, G.W. Herschman*
- Provider signature guidelines and solutions: Autograph please! Dec, p. 10; *J. Marcus*
- Physician compliance education outside of the hospital environment. Dec, p. 26; *K.R. Earp*
- Patient visits: Reforms increase provider responsibilities. Dec, p. 42; *A. Miller*

Quality

- Changing the execution gap: Quality Improvement Action Planning.™ March, p. 39; *B. Chapman, R.C. Bennett*
- Acquittal of Texas nurses who reported physician standard-of-care concerns. June, p. 28; *J.B. Killgore, J.A. Anderson*
- Opportunity knocks for hospital boards to impact clinical quality. July, p. 6; *J.A. Anderson, C.J. Hannagan*
- Quality improvement takes on new imporn tance in health care organizations. Sept, p. 23; *F. Nigrello, G. Kaufman*
- Using client grievance data to proactively improve quality of care. Oct, p. 38; *S.M. Chisholm, B. Blue*
- Fraud in quality measurement and reporting: The physician compliance challenges. Nov, p. 8; *D.F. Shays*

Research

- Common compliance problems in human subject research. Jan, p. 20; *E. Paal*
- FDA issues guidance for investigators in clinical trials. April, p. 8; *K. DeVille*
- Research compliance: PhRMA guidance on professional conduct in clinical trials. May, p. 38; *S. Parsley*
- Internal monitoring of human subjects research: Why take the initiative? June, p. 45; *M. Wheeler*
- Research consents and patient medical records: Requirements and best practices. Aug, p. 22; *D. Vulcano*
- Empathic research compliance: The research admin and PI perspectives. Sept, p. 36; *M.B.J. Chun*
- Research compliance in a changing world. Oct, p. 36; *L. Harris*
- Assessing and managing research compliance risks in the health care setting. Nov, p. 20; *J.M. Campbell*
- Gaps in FDA oversight of the financial interest of clinical investigators. Nov, p. 44; *B. McDowell*

Social Media

- Social media at work: The rules of engagement. June, p. 20; *S. Lee*

Social Networking by John Falcetano

- Topics for newcomers. Jan, p. 17
- CHC certification. Feb, p. 17
- Blog postings. March, p. 19
- Academic medical center staffing. April, p. 21
- Setting up an online group. May, p. 48
- Topics and documents. June, p. 17
- Discussion groups. July, p. 19
- Faxing PHI. Aug, p. 19
- Documents and discussion topics. Sept, p. 19
- Compliance Communities. Oct, p. 19
- Dashboard. Nov, p. 49
- Employee hotline. Dec, p. 13

Surveys

- The evolving role of the chief compliance and ethics officer: A survey by the HCCA and SCCE. Dec, p. 24; *A. Turteltaub*

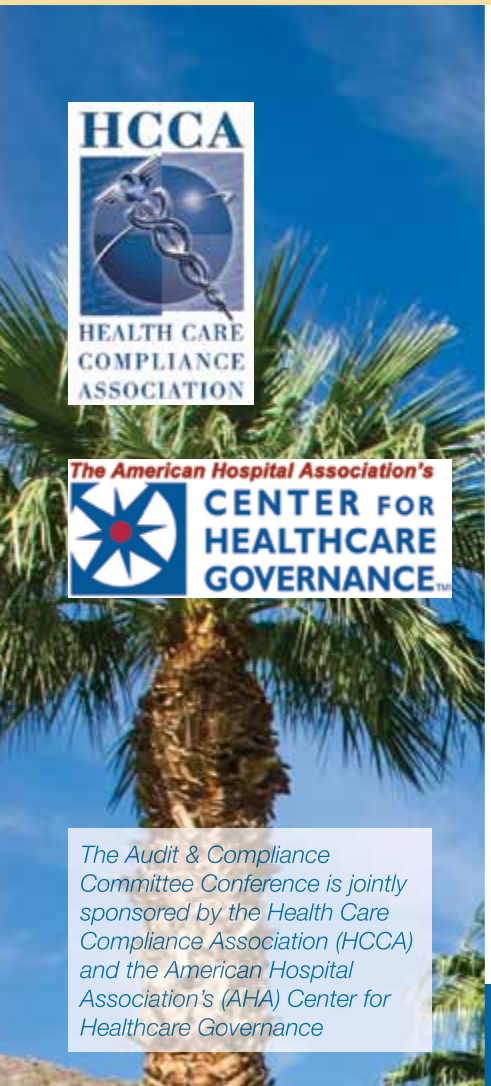
Managed Care
Compliance Conference

February 6–8, 2011
Scottsdale, AZ

General Sessions:

- Hot Topics from CMS Staff
- Health Care Reform Panel: How My Plan Is Dealing with HC Reform
- How the SIU Unit Works with Compliance
- Case Studies: Breach Notification Compliance—The Feds Are Watching

LEARN MORE AT WWW.HCCA-INFO.ORG



The Audit & Compliance Committee Conference is jointly sponsored by the Health Care Compliance Association (HCCA) and the American Hospital Association's (AHA) Center for Healthcare Governance

Improving Governance Practices

Audit & Compliance

COMMITTEE CONFERENCE

BUY ONE registration for $695 and **GET ONE** for $395

February 7–8, 2011 | FireSky Resort & Spa, Scottsdale, AZ

What You'll Learn:

- The Impact of Health Care Reform on Regulatory Risk and Compliance Obligations
- Fulfilling Your Fiduciary Obligations as Board Members
- Improving Your Board Performance

Session Topics:

- Enforcement Actions
- Introduction to Healthcare Risk Areas & Compliance
- Fiduciary Duty, Corporate Scandals
- Committee Charter: The Role and Responsibility of the Audit and Compliance Committee
- Internal Audit and the Audit Committee
- External Audit and the Audit Committee
- Enterprise Risk Management Risk Assessments and Internal Controls
- Case Study in Crisis Management

LEARN MORE AT www.auditcompliancecommittee.org