HCCA

HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY

Volume Thirteen
Number Eleven
November 2011
Published Monthly

Meet

Dwight Claustre, Long-time HCCA Compliance Institute enthusiast

PAGE 15

Earn CEU Credit

WWW.HCCA-INFO.ORG/QUIZ—SEE PAGE 68

Feature Focus:

Civil and criminal liability for overpayments

PAGE 26

Will the SEC's whistleblower bounty change employer/employee relationships?

PAGE 44

INSIDE PAGES PRINTED ON 100% RECYCLED PAPER

SEE PAGE 55

Global Compliance: *Good for Business*℠

We've taken the guess work out of building and maintaining an effective risk reduction program by integrating our full suite of proven and field-tested services. Over 800 health care organizations are currently utilizing our expert solutions and insight to protect their organizations.

- Hotline Solutions
- Training & Education
- Expert Advice
- Performance & Benchmarking

Learn more about our complete ethics and compliance solutions. Contact us today at **800-876-5998** or **contactus@globalcompliance.com.**

GLOBAL COMPLIANCE™
Good for Business.

www.globalcompliance.com

INSIDE

4 **Are we having fun yet? CMS posts new 855 enrollment applications**
By Anna Grizzle, Claire Miley, and Seth Killingbeck
Tips for dealing with revisions in the Medicare enrollment and revalidation process.

12 **CEU: Pitfalls of and lessons learned: Provider documentation in the EMR**
By Ruth Krueger
Time-saving tools for recording patient encounters can be a blessing or a curse.

15 **Meet Dwight Claustre, Long-time HCCA Compliance Institute enthusiast**
An interview by Debbie Troklus

18 **Newly Certified CHC®, CHRC®, and CHPC®**

20 **Letter from the CEO** By Roy Snell
Conflicts of interest

21 **Social Networking** By John Falcetano
You don't have to be quiet in this library

22 **Exhale** By Shawn DeGroot
Walk the talk

26 **Feature Focus: Civil and criminal liability for overpayments**
By Gabriel L. Imperato
It's more important than ever that procedures for reporting and refunding overpayments are up to date.

29 **CEU: They will never remember the vendor; you, however, are unforgettable...**
By Laurie Smaldon and Gretchen Hood
Aggressively managing vendors and business associates to avoid data security breaches and protect your brand.

35 **Joshua's Law: Patient privacy**
By Christopher R. Gingras
Social media policies must include clinically appropriate use of photos and videos of patients.

39 **Compliance 101: Review of compliance fundamentals**
By Alexandra F. Holt
A half-baked compliance program won't do in today's environment of ethical and behavioral challenges.

44 **CEU: Will the SEC's whistleblower bounty change employer/employee relationships?**
By David Restaino
It's time to refocus internal compliance programs to prevent damage as whistleblowers look for opportunities.

48 **Evolution of a compliance plan: Protecting revenue**
By Susan Theuns
Look for areas where your compliance program is costing you time and money, and areas where money could be made.

52 **In search of: The excluded**
By Martha Ann Knutson
Thorough, periodic screening for excluded individuals and companies will safeguard your business.

56 **Mentoring**
By Marcella Henry
A look at how an experienced mentor can guide a "newbie" to develop an effective compliance program.

57 **People on the Move**

59 **Dodd-Frank: Much ado about nothing? A survey by HCCA and SCCE**
By Adam Turteltaub
The impact of the Act's whistleblower provisions on compliance programs appears to have been minimal.

62 **HCCAnet and Website News**

66 **New HCCA Members**

Are we having fun yet? CMS posts new 855 enrollment applications

By Anna Grizzle, Esq; Claire Miley, Esq; and Seth Killingbeck, Esq.

Editor's note: Anna Grizzle and Claire Miley are Members, and Seth Killingbeck is an Associate of the Bass, Berry & Sims PLC Healthcare Industry Practice area in the law firm's Nashville offices. Anna may be contacted by phone at 615/742-7732 or by e-mail at agrizzle@bassberry.com. Claire may be contacted by telephone at 615/742-7847 or by e-mail at cmiley@bassberry.com. Seth may be contacted by telephone at 615/742-7707 or by e-mail at skillingbeck@bassberry.com.

On July 5, 2011, the Centers for Medicare & Medicaid Services (CMS) posted new versions of the Medicare enrollment applications, or 855s, on its website. Although CMS has been slow to publicize these new applications, some of the changes may significantly impact Medicare providers and suppliers. The revised 855s, coupled with the recent announcement that CMS will require most current Medicare providers and suppliers to revalidate their enrollment information between now and March 2013, will make the already challenging Medicare enrollment process even more daunting. This article discusses key revisions to the 855s, anticipated impacts on the provider and supplier community, and tips for providers and suppliers navigating the enrollment and revalidation process.

The new enrollment applications

In the months leading up to the publication of the new 855s, CMS quietly submitted drafts of the revised applications to the Office of Management and Budget (OMB) for review, but did not widely broadcast its intention to revise the applications. In fact, provider enrollment representatives at certain Medicare contractors have, during informal conversations, indicated that they did not learn of the new 855s until after CMS had published them on its website. Further, some provider enrollment representatives have indicated that the Medicare contractors first learned of the new applications when providers and suppliers called with inquiries—not from announcements or guidance from CMS. On August 23, 2011, approximately seven weeks after posting the forms on its website, CMS finally made a public announcement, via its e-mail listserv to fee-for-service providers, that the new 855s are available on the website. In its listserv announcement, CMS encouraged providers and suppliers to use the revised 855s, but indicated that the old forms may be used through October 2011.

All 855 enrollment applications now bear an effective date of July 2011. Of the revised 855 forms, the most substantial changes have been made to the Form 855A (for institutional providers), but CMS also revised the Form 855B (for clinics/group practices and certain other suppliers), the Form 855I (for physicians and non-physician practitioners), the 855R (for reassignment of Medicare benefits), and the 855S (for durable medical equipment, prosthetics, orthotics, and supplies [DMEPOS] suppliers). In addition, CMS introduced a new Form 855O, which will be used by physicians and non-physician practitioners (NPPs) who enroll for the sole purpose of ordering or referring items for Medicare beneficiaries. Note that many of the changes made to the 855s are formatting changes, but certain of the substantive changes, mainly with respect to the 855A, may significantly increase the burden associated with obtaining

and maintaining enrollment in the Medicare program.

Changes applicable to all institutional providers

Form 855A is the Medicare enrollment form used by institutional providers, including hospitals, skilled nursing facilities, home health agencies, hospices, rural health clinics, end-stage renal disease facilities, comprehensive outpatient rehabilitation facilities, and certain other providers. Among the more significant changes to the disclosures required by all institutional providers on the new 855A are:

- Providers must indicate in Section 2.A.4 whether they are physician-owned hospitals.
- Providers must report whether they are proprietary or non-profit and their year-end cost report date in Section 2.B.1.
- For providers organized as limited partnerships, limited partnership interests need to be reported only if the interest is at least 10% (a welcome liberalization of the former commonly accepted interpretation that all limited partnership interests, irrespective of percentage, must be reported).
- Organizations and individuals with an ownership interest or managing control must report their "exact" percentage of ownership in the provider in Section 5 and Section 6, respectively.
- Organizations with an ownership interest or managing control must indicate whether they were "solely created to acquire/buy the provider and/or the provider's assets."
- Organizations with an ownership interest or managing control must indicate their type of organization in Section 5 (e.g., holding company, medical staffing company, investment firm, etc.).
- Organizations and individuals with an ownership interest or managing control must indicate in Section 5 and Section 6 what type of contractual services (if any) they provide to the enrolling provider.
- Providers must submit an organizational diagram identifying all of the entities listed in Section 5 (organizations with an ownership interest and/or managing control) and their relationships with the provider and with each other. If the provider is a skilled nursing facility, the provider must submit a diagram identifying the organizational structures of all of its owners, including owners that were not required to be listed in Section 5 (organizations) or Section 6 (individuals); and
- Section 17 makes it clear that the Medicare contractor "may request, at any time during the enrollment process, documentation to support or validate" information reported in the 855, including documents not specifically requested on the application form.

Given the specificity of the information that must now be reported in the 855A, the new 855A has the potential to significantly increase the burden on providers to obtain and maintain their Medicare enrollment. For example, given the precision with which ownership interests must be reported, it is unclear whether CMS will expect providers to submit an 855A change of information to the contractor each time an ownership percentage fluctuates. If so, this would prove particularly burdensome—if not unrealistic—for providers owned by publicly-traded companies, where ownership levels change continually. Furthermore, it is unclear whether CMS will expect providers to submit a change of information each time the nature of contractual services provided by an organization or individual with an ownership interest or managing control changes. Given the ambiguously broad reach of these disclosures, CMS will hopefully provide additional guidance to the provider community as well as to CMS' contractors.

Changes specific to physician-owned hospitals

One of the main factors presumably driving the development of the

Continued on page 7

Look past risk and see clear to opportunity.

When you're forced to rely on labor-intensive spreadsheets, point solutions, or a complicated software system retrofitted to the healthcare industry, it can feel as if your risk is managing you.

Go beyond risk management to continuous improvement with a customized, scalable and complete solution, fully supported by experts in the healthcare compliance industry.

MediRegs provides you with the tools you need to proactively assess, understand, communicate and mitigate risk across your entire enterprise.

Visit **MediRegs.com/ERM** today to see why our customers prefer our solution for enterprise compliance and risk management.

ComplyTrack™ delivers solutions for:

- Compliance
- Risk
- Health Information Management
- Audit & Compliance Committee
- Privacy & Security
- Legal
- Internal Audit

Wolters Kluwer
Law & Business

new 855A is Section 6001 of the Patient Protection and Afford able Care Act (PPACA), which amends the whole hospital exception to the Stark Laws. The amended whole hospital exception effectively prohibits the formation of new physician-owned hospitals and prevents any increase in the level of physician ownership of existing physician-owned hospitals. To this end, it requires all Medicare-enrolled hospitals to disclose to CMS whether they have physician owners and, if so, information regarding those physician owners. Accordingly, Section 2 of the 855A now requires the applicant to indicate whether it is a physician-owned hospital. The 855A defines a physician-owned hospital as

> any participating hospital in which a physician, or an immediate family member of a physician has an ownership or investment interest in the hospital….through equity, debt, or other means, and includes an interest in an entity that holds an ownership or investment interest in an entity that holds an ownership or investment interest in the hospital.[1]

A physician-owned hospital must complete the new Attachment 1 to the 855A, which consists of two sections. Providers who do not have physician ownership are not required to complete Attachment 1.

Section 1 of Attachment 1 must be completed for every *organization* that has *any* percentage of ownership or investment interest in the physician-owned hospital. Similarly, Section 2 of Attachment 1 must be completed for every *individual* who has *any* percentage of ownership or investment interest in the physician-owned hospital. This standard is different than Section 5 of the 855A, which generally requires the reporting of owners (with the exception of general and limited partners as described above) only if they have a direct or indirect ownership interest *of at least 5%.* Section 1 and Section 2 of Attachment 1 require the submission of information regarding these owners, including the owner's:

- Full legal name
- Address
- Medicare identification number and National Provider Identifier (NPI), if applicable
- Effective date of ownership interest
- Percentage of ownership interest (reported to two decimal places), and
- History of certain reportable final adverse legal actions

Section 1 of Attachment 1 does not expressly state that *organizations* with an *indirect* ownership interest in a physician-owned hospital must be reported, so presumably only direct ownership interests must be reported for organizations. Please note that this comment applies only to Attachment 1. Providers must still report both direct and indirect ownership by organizations that equals or exceeds 5% in Section 5 of the 855A.

In contrast to Section 1 of Attachment 1, Section 2 of Attachment 1 states that all *individuals* with any direct or *indirect* ownership in a physician-owned hospital must be reported in Section 2. Specifically, along with all physicians and immediate family members of physicians who have a direct or indirect interest in a physician-owned hospital, CMS requires "[a] ll individuals who are not physicians or immediate family members of a physician, but who have a direct or indirect ownership interest or investment interest in a physician-owned hospital" to be reported in Section 2 of Attachment 1.[2] CMS then gives the following example: "Nancy Jones, a teacher, has a 2% direct ownership interest in a physician-owned hospital. Ms. Jones's ownership interest must be reported in Attachment 1, Section 2." Based on CMS' broad language requiring disclosure of all individuals' direct and indirect ownership interests, Ms. Jones's ownership arguably would need to be reported even if her ownership or investment interest in

Continued on page 9

MANAGE CLAIMS AUDITS WITH TOTAL CONFIDENCE. Multiple audits, hundreds of claims, dozens of team members, zero free time. Miss one date and you forfeit hard-earned revenue. With so much complexity – and so much at stake – only Compliance 360 offers the confidence of a 24x7 Virtual Audit Coordinator that manages every step of every audit in one central system. No gaps, no guesses, no gotchas.

Visit www.compliance360.com/ClaimsAuditor to learn how we're helping thousands of providers protect their revenues – and their peace of mind. **GET THE 360° VIEW**.

www.compliance360.com

Compliance 360°

 ...continued from page 7

the physician-owned hospital is indirect (i.e., if Ms. Jones owns stock in a company that operates physician-owned hospitals). If this is really CMS' intention, then the Attachment 1 disclosures may present a formidable challenge to many physician-owned hospitals. Hopefully, CMS will provide additional guidance to clarify (and narrow the scope) of this disclosure requirement.

Forms CMS-855B and CMS-855S

Although most of the revisions to the remaining 855 forms were cosmetic changes, CMS did make some substantive changes. For example, the 855B now requires the supplier to report whether it is proprietary or non-profit. In addition, both the 855B and 855S require the supplier to disclose the state and country of birth for individuals reported in Section 6 as having an ownership interest or managing control in the supplier.

Form CMS-855O

The 855O is a relatively short enrollment application, consisting of only six sections and 13 pages. The application, which is to be completed only by providers or non-physician practitioners (NPPs) who will order or refer Medicare items or services but not submit claims to Medicare, asks for only basic information about the provider or NPP. For example, the provider or NPP must provide basic identifying information, contact information, professional licensure and credentialing information, and a description of any adverse legal history.

Request for revalidations

Revalidation is a process by which a Medicare provider or supplier recertifies the accuracy of its enrollment information by submitting a complete 855 application. Although Medicare revalidations are generally not required more frequently than every five years, CMS has authority under 42 CFR 424.515(d) to request "off-cycle" revalidations in certain situations.

On August 8, 2011,[3] CMS announced that it will require all providers and suppliers who enrolled in Medicare prior to March 25, 2011 to revalidate their enrollment under the new enrollment screening criteria imposed by Section 6401(a) of PPACA. CMS' contractors will request these revalidations by March 23, 2013. Newly enrolled providers and suppliers who submitted their enrollment applications to a CMS contractor on or after March 25, 2011 will not be required to submit these off-cycle revalidations.

CMS has instructed providers and suppliers that they should wait and submit the revalidations only after being asked to do so by their respective Medicare contractors. Once a provider or supplier receives a revalidation request from its Medicare contractor, it will generally have 60 days from the date of the request letter to submit complete enrollment forms. Failure to submit the enrollment forms as required may result in the deactivation or revocation of the provider's or supplier's Medicare billing privileges. As a result, providers and suppliers may wish to ensure that all of their practice locations (and not just their "official" correspondence address on the 855) can receive and forward mail for proper handling. There have been informal reports of revalidation requests being sent not to the official correspondence address, but to practice locations.

Unless a provider or supplier qualifies for a hardship exception, a revalidation submitted by a provider or supplier (excluding physicians, NPPs, and physician and NPP organizations) must be accompanied by an application fee, as required by PPACA. For calendar year 2011, the application fee is $505.

What providers and suppliers can do now

Providers and suppliers should become familiar with the new 855s as soon as possible, because the new forms may require significant additional disclosures,

Continued on page 10

 ...continued from page 9

although providers and suppliers will not be required to use the new 855s until November 2011. We also recommend that providers and suppliers immediately begin to gather the information that will be required to complete the applicable 855. For some providers and suppliers, this will involve preparing organizational diagrams to submit to a Medicare contractor and/or gathering detailed information about all organizations and individuals who have an ownership interest or managing control in the provider or supplier. Providers and suppliers should also understand what documents, such as state operating licenses, may need to be included with the 855 as part of a revalidation. By preparing this information now, providers and suppliers will find themselves in a much better position when (not if) they receive a mandatory revalidation request from a Medicare contractor and the 60-day clock begins to run.

Because of the limited time afforded a provider or supplier to respond to a revalidation request and because of the potential of deactivation or revocation of Medicare billing privileges for noncompliance, we recommend that providers and suppliers incorporate Medicare enrollment into their compliance plans. For example, a compliance plan may include the process for logging, handling, and responding to a request for revalidation to ensure that the provider or supplier responds to the Medicare contractor in a timely manner. A compliance plan might also outline how information regarding owners is maintained and how changes are reported to CMS contractors in a timely manner. ■

1. See Section 2, "Special Enrollment Notes," p. 9 of CMS-855A (07/11).
2. See Attachment 1, Section 2 instructions, p. 56 of CMS-855A (07/11).
3. See MLN Matters Number SE1126 (August 8, 2011). A revised MLN Matters Number SE1126 was published on August 10, 2011, and corrected the PPACA citation from Section 6401(d) to 6401(a).

Streamline workflow
Enhance compliance
Reduce costs

MediTract helps healthcare organizations manage intricacies of the **HITECH Act** so they can focus on their primary objective – providing the highest levels of patient care.

MediTract's Contract Management Solution increases profits and productivity while helping healthcare organizations manage business associate agreements, track and monitor compliance regulations associated with physician contracts and reduce the risk of disclosure of information to unauthorized parties.

- Comprehensive management of BAAs
- Enhance Compliance
- Centralized, secure database

MediTract® is the leading technology-based contract management service provider in healthcare serving more than 1,600 healthcare organizations in over 5,900 locations across the United States.

MEDITRACT®

Changing the Way Healthcare Does Business™

www.meditract.com
(877) 492-8490

Pitfalls of and lessons learned: Provider documentation in the EMR

By Ruth Krueger MS, RRT, CHC

Editor's note: Ruth Krueger is Regional Director of Corporate Compliance at Sanford Health in Sioux Falls, South Dakota. Ruth may be contacted by telephone at 605/328-6681 or by e-mail at Ruth.Krueger@sanfordhealth.org.

Physician documentation in the electronic medical record (EMR) is both a blessing and a curse. Used appropriately, documentation efficiency tools, such as copy forward, templates, note consolidation, and voice recognition, can be real time savers. That's one of the blessings. When these tools are used inappropriately and without editing, the blessing turns into a nightmarish curse—one that can place your facility/clinic at high risk for fraudulent billing. I'm sure I speak for many compliance officers when I say that if we could go back in time to when our systems began planning for the EMR and developing the training curriculums, we would take a much stronger stand related to the use of these efficiency tools.

What can we do now? Here are some key points to reinforce with all providers;

- The medical record is used not only to document the care that is provided to the patient, but also to support payment for the services provided.
- The entries in the record must be accurate, concise, and complete to explain the patient's current state. The documentation must reflect the physicians' actions and decisions as they care for the patient.
- The EMR must clearly describe the patient's clinical condition for that visit, the reason for the care, and the necessity of the visit, hospitalization, procedures, and treatment decisions.
- Copying information from another source into a note must be done with great caution. The EMR eliminates legibility problems, which in turn alleviates stagnant or erroneous information.

The following risk areas need focused attention to help assure that the provider documentation reflects the care provided.

Copy/Paste/Copy Forward

When providers copy-and-paste or copy forward a previous encounter without editing, they are showing the work they did on a previous encounter, not the work done on the current visit. The information copied may be outdated or conflict with other information that is documented on the current visit. This puts the coder in a difficult position, when he/she must weed through the documentation to decipher the care provided or query the physician to clean up that documentation so the appropriate level claim can be billed. Either way, it is a resource burn that would be avoided if the documentation was edited by the provider. Providers using the copy forward function must have a complete understanding that they must edit what is copied and identify any copied text to the appropriate author. Intentional use of another provider's note without acknowledgement and editing may be considered fraud and abuse. Copying another's work without crediting the author is plagiarism.

Templates

Template use may be even more onerous than the copy function and can lead to note bloat. With pre-populated templates, coders and payers are unsure that the billing provider did everything documented. Payers will deny claims when templates are used that do not reflect the care provided (e.g.,

a breast and pelvic exam documented because the wrong template was pulled for a male patient). Many EMR systems allow the physician to develop their own templates, which leads to problems if the provider isn't thoroughly trained to understand the risk when using those templates. Payers are cautioning against claim submission with documentation that isn't patient-and date of service-specific. Auto-populated paragraphs can provide useful information, such as the etiology, standards of practice, and general goals of a particular diagnosis. The problem is, they are generalizations and do not support medically necessary information that correlates to the management of the particular patient. Payers are seeing the same auto-populated paragraphs in the histories and physicals of different patients and are denying claims for that reason.

Note consolidating function

Use of this function (also known as note integration) may be problematic when the nurse begins the encounter by filling in all the initial assessment information plus pulling in previous information. The provider then takes the nurse's note as his/her own and uses that information in the documentation. The provider must verify and edit the information that the nurse entered, add his/her specific information for the encounter to be billed, and then choose the function that then makes that note the provider's note. If they fail to click that button, there is no documentation from the provider—only the nurse's note—which renders that encounter unbillable.

Voice recognition

Transcribing recorded notes with voice recognition is a great tool to speed documentation, but only great if the speech is clear and has little or no background noise. Typically, the more this function is used by the provider, the better the system is able to recognize his/her individual voice and accurately type the notes. Again, editing is the key. The provider must edit the voice notes to ensure that the words typed are what were intended.

Continued on page 14

 ...continued from page 13

Medical student documentation
Medicare does not pay for any services furnished by a medical or other student. An essential part of med student education involves learning how to document patient care in the medical record. Students may document in the EMR, but for the evaluation and management (E/M) service, the physician may only refer to the student's review of symptoms (ROS) or past family social history (PFSH).

Residents
Residents may document all of the care of the patient when under the teaching physician's supervision. If the physician is not present when the resident evaluates the patient, that physician must perform a separate face-to-face encounter with the patient to confirm the resident's information. The physician doesn't need to re-document everything the resident did, just confirm the information and indicate that they both participated in the management of that patient.

Summary

The EMR has many benefits over the paper chart. EMR entries are always legible, they are always dated and timed, and they are accessible from many entry points. The EMR and documentation support tools are designed to improve patient care and safety. These features can save providers time by providing easy access to masses of information, but they do not necessarily save time in the providers' day-to-day entry of patient encounter notes. If providers aren't careful, this is what leads them down the path of shortcuts to improve their efficiency. I'm certain we all have many great examples of physicians in our systems who are appropriately using the efficiency tools available in the EMR. Proper use is the habit that must be adopted—one to which we must insist that our providers adhere. Use your good documenters and appropriate tool users to show other providers how it can be done. Provide those bad examples (de-identified of course) to your providers to show how the tools are used inappropriately.

Recommendations for documentation improvement

- Develop a policy that defines the provider documentation responsibilities and share it with all players.
- Design a process for coders to follow when errors are noted and ensure that the first step is letting the providers know what they are doing wrong. This sounds simple, but this is a step that is missed many times.
- Educate all players on the process and share the poor documentation examples with your management team, along with any claim paybacks or denials associated with poor documentation.
- Set up a prospective work queue for coders/compliance professionals to review and validate patient encounter EMR files of providers who are poor documenters.
- Encourage the use of a compliance professional or a coding manager to sit with problematic providers to show them where they go wrong.
- Engage your physician champions/leaders and executive management in the process and escalate all continued problems to them to manage one-on-one with provider.
- Tie sanctions to those providers with poor documentation habits. Hint: Fines don't usually work—suspension usually does.

When you engage your information technology (IT) trainers for the EMR, physician leadership, and executive management, you raise the bar with the expectation of progress in improving documentation while still using the efficiency that the EMR tools afford. Addressing these issues with strong direction from Compliance will assist with improving documentation, so that claims go out the door with the documentation reflecting the services that were provided.

For more information on this topic, an excellent read is the AAMC White Paper EHR Documentation from July 11, 2011 (available at https://www.aamc.org/download/253812/data/appropriatedocumentationinanehr.pdf) ■

feature article

Meet Dwight Claustre

Long-time HCCA Compliance Institute enthusiast

Editor's note: This interview was conducted in September 2011 by Debbie Troklus, CHC-F, CCEP-F, CHRC, CHPC, member of the Health Care Compliance Association Board of Directors and President of the Compliance Certification Board. Debbie Troklus may be contacted by e-mail at dtroklus@meaderoach.com and Dwight Claustre may be contacted by e-mail at bdwightclaustre@yahoo.com.

DT: Dwight, please tells us a little about yourself, your background, and how and when you got started in health care compliance.

DC: I am officially a Medicare beneficiary. I've been married for 42 years, have one daughter, three grandchildren, and one on the way. Health care is my second career. My first career was law enforcement. I spent 13 years as a police officer in Michigan, before entering health care.

I have been in health care for 32 years. Twenty of those 32 years were spent with Catholic Healthcare West (CHW), a 40-hospital system based in San Francisco. Much of my career was in risk management and operations. In 1996, I was designated as the Regional Compliance Officer and in 2001, I took a corporate position as the System Director of Compliance. This was really the beginning of what has been a very rewarding compliance career. This is where I met my true mentor Dan Roach, Vice President Compliance and Audit for CHW.

I retired from CHW after 20 years and decided to try my hand at consulting. One of my first assignments was as the Interim Chief Compliance Office for a children's hospital in California. I quickly realized that I enjoyed and missed the hospital atmosphere, with more involvement in operations. I decided to leave consulting after a year and focus on filling interim compliance positions as an independent contractor.

DT: What is your current job?

DC: I am presently an independent contractor working for Sutter Health, a California-based health system. I am working for Steve Ortquist in the Ethics and Compliance department. I am using my experience to help Steve with special projects.

DT: How soon after first getting into health care compliance did you join the Health Care Compliance Association and why?

DC: It was almost immediately. I

Continued on page 16

believe I joined in 2001. I joined for several reasons: (1) It was the only organization that, at the time, was dedicated to the health care compliance profession; (2) I needed the resources that HCCA provided to begin to learn a new profession. While I had a good understanding of health care and operations, the specific knowledge base for compliance was new to me as well as new to health care; and (3) It was an opportunity to network with people in the same profession, both new to the profession as well as seasoned veterans.

DT: When did you first attend an HCCA Compliance Institute (CI) and why?

DC: I believe my first attendance was in either 1998 or 1999. I attended what, at the time, was an early Institute in Phoenix, Arizona. It was an opportunity for me to begin to learn about this thing called "health care compliance" without the cost of traveling. At the time, I was the designated Regional Compliance Officer for a Phoenix-based hospital and really didn't know what all it entailed. Actually, at the time, I really hadn't heard much about HCCA, which was still in its infancy. I remember meeting Paul Belton, the now Vice President Compliance for Sharp Healthcare in San Diego. This was the beginning of our personal and professional friendship. It is these types of relationships that continue to make HCCA a valuable commodity.

DT: Thinking back to that first CI you attended, what information or new contact was it that helped you when you returned to your work, and why did you return to the CI the following year?

DC: The first real full Institute I attended was in 2002. I was still considered a rookie to the field of Compliance. I remember coming back to work and thinking, "Oh my goodness we have so much work to do." Back then, there was certainly a focus on Medicare and billing. People were beginning to talk about Stark, but there wasn't the government focus there is today. I met so many people that first year, I don't remember anyone specifically. But, I do remember sitting around with groups of colleagues wide-eyed with the concerns of all the work that was needed in all our organizations to not be the headline in the local newspaper. I returned the following year to gain a greater understanding of the profession, of the issues, and for the networking with colleagues and friends. While some of us would talk during the year, many of us would only have contact at the Institutes. But, it was an advantage to have people in the business that you could call to discuss concerns and possible fixes. One of the most important documents I take away from the Institutes is the list of attendees.

DT: What is it about the CI that has brought you back to it year after year?

DC: The Compliance profession is ever changing and ever growing. There are always new issues and new or better processes to attack the issues. The government, over the years, has increased its focus on health care fraud and abuse. Stark has become what I consider to be one of the major risks in health care today. The need for networking with and interaction with colleagues is an important factor in my continued attendance at the Institutes. While I consider myself to be a seasoned compliance professional, I am in no way an expert. I always come away with something I can bring back to my organization, whether it is a new concern, or focus, or a best practice. I hope that I am being a mentor and provide valuable knowledge to new compliance professionals who come to the Institutes. It was in 2005 that I first became a presenter at the Institute, and I have continued that through the years.

DT: If a compliance colleague asked you if and why they should attend the 2012 Compliance Institute, what would you tell them?

DC: I would tell them they can't afford not to. I know it is time consuming and costly in today's environment, but the diversity of sessions gets better every year. HCCA is now providing sessions for the seasoned veteran who can

still learn something new, and sessions for the person new to compliance and to HCCA. The industry-specific sessions offer the individual an opportunity to network with people within their same business. The speakers, with varied backgrounds and experience, provide tools and knowledge for the compliance professional to take back to their organizations. Not only do you learn best practices, but you build lifelong friendships, which makes it well worth the time to attend the Institute. The Institute also provides the opportunity for the compliance professional to have access to a variety of vendors in the compliance arena.

DT: Do you feel that the resources that the HCCA provides have assisted you in the Compliance profession over the years, and if yes, which ones and why?
DC: I definitely believe that the resources that HCCA provides have been beneficial to my career. As I think about which ones, several come to mind. First, and not in any specific order, is the **Compliance Today** publication. I know it isn't easy to get writers and put it together month after month. But again, I always take something new away from the readings. The diversity of the articles benefits everyone, whether from a small community hospital to a large academic medical center. Secondly, fairly new, social media-type communications that allow people to network with such a wide range of individuals. Lastly, because of the reason previously discussed, nothing has been more beneficial than the Institute with its educational and networking opportunities.

DT: What other HCCA programs and services have you participated in over the years?

> One of the most important documents I take away from the Institutes is the list of attendees.

DC: In 2003, I co-chaired what was then the HCCA West Regional. I remember we wanted to hold it in Las Vegas and there was concern, at the time, with holding an HCCA function in Las Vegas. Roy Snell agreed, and we had 150 people attend. It was the best turnout for a regional conference. I have continued to chair the West Regional since that time. I have attended the Physician Practice Conference as well as the Quality conferences.

I remember a Physician Practice Conference in San Francisco. During the night of the first day, there was a storm that knocked out the power to the hotel. The next day, we had to complete the conference by candlelight.

Later, I began to focus on research compliance and began attending the HCCA Research Conferences, and now I am a presenter for the conference. I was asked to participate in the writing of the test for the Research Compliance Certification, and I am now one of the faculty at the Research Academies.

I also attend the AHLA/HCCA Fraud and Abuse Conference on an annual basis. As you can probably surmise, I am a believer in education. For me, it is easier and more beneficial to do it through formal programs, such as the Institute. This has been true throughout my entire career in both law enforcement and health care.

DT: Are you Certified in Healthcare Compliance (CHC)? If so, why did you seek certification?
DC: I am certified and have been for seven years. I believe being certified indicates to employers and to colleagues that you have taken the time and effort to learn beyond the basics. It is also a personal satisfaction to know that you are among the other professionals who have achieved the certification. I am also Certified in Healthcare Research Compliance (CHRC).

DT: Do you feel that the certifications are important for compliance professionals to obtain?
DC: We are seeing more and more ads for compliance professionals requiring the applicant to either have the CHC or obtain

Continued on page 18

Meet Dwight Claustre, Long-time HCCA Compliance Institute enthusiast

...continued from page 17

it within a specified time period. To a great degree, obtaining the certification becomes a personal challenge and satisfaction. If you are fairly new to the profession, the preparation is an education in and of itself. So, yes I think it would be beneficial to the compliance professional.

DT: As you think ahead to the 2012 Compliance Institute, what is it you are most looking forward to?

DC: The 2012 Institute is probably going to be my last Institute as I look forward to entering the world of retirement. So, I will look forward to seeing many of my friends and colleagues at an Institute for the last time. Although it will be my last, I will still be enthused about continuing to learn. As I indicated earlier, I always take away something new. I will continue to network for my benefit as well, hopefully, for the benefit of others. I am going to be a presenter at the conference. I want to thank HCCA for all they have provided me over the last 10-plus years. I always look forward to the Institutes. ■

The 2012 Compliance Institute Preliminary Brochure is now available online. Visit www.compliance-institute.org to download the brochure and to register.

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.

Congratulations!! The following individuals have recently successfully completed the CHC® certification exam, earning their certification:

Eileen C. Addison
Ann M. Amato
Marianne Bechtle
Theodore J. Bliman
Craig J. Brandt
Beverly Brouse
Michelle E. Calloway
Ruth E. Cardiello
Karen Carey
Kevin W. Carlson
Stacey L. Carr
Bernadette Catanzaro
Marilyn B. Chew
David H. Chin
Ronda K. Cross
Ed Crowe
Philip J. Curran
Melissa F. Dejohn
Lia Faraclas
Nancy Fletcher
Dadrion A. Gaston
Heather D. Gatton
Sandra D. George
Jim Harner
Charles E. Harrison
Laura K. Hartsock
Stephanie Z. Haywood
Ashlie S. Heald
Sonya L. Henderson
Sheila J. Henson
Jennifer Hutton Slaise
Shelley R. Johnson
Jennifer L. Jones
Luis A. Jusino
Teresa L. Knox
Kathy Kotin
Richard Leboutillier
Joshua L. Malone
Cynthia M. Marsh
James Massey
Michelle L. Matricardi
Martin S. Merlotto
D'Andrea J. Morning
Lina Pacelli
John L. Petrosino
Andrea G. Phillips
Vanessa Ramirez
Natalie C. Sharpe
Philip W. Sherfey
Mara Sierchio
Laurie A. Smaldon
Eugenia F. Smither
Nelly D. Stone
Kimberly M. Thomas
Amy S. Tolliver
Brenda Tranchida
Josh M. Troop
David V. Way
Candice M. Weatherly
Kelly M. Willenberg
Anahita Yousefiani

Congratulations!! The following individuals have recently successfully completed the CHRC® certification exam, earning their certification:

Claire F. Agnew
Myrna L. Arvizo
Kerry D. Borawski
Eva A. Branch
Sharmila M. Chandran
Vicki Ann Clevenger
Christine Cramer
Richard J. D'Augusta
W. Michelle Fronheiser
Hana Gragg
Karl E. Green
Crystal E. Gruetzmacher
Lory Ann Hayes
Debra Hinson
Donna J. Hoagland
Cr Matthew Hodgson
Maria A. Joseph
Elimu Etumba Kajunju
Ellen Kapsalis
Henri-Alexandre N. Lauer
Patricia A. Marshall
Jennifer McCafferty
Helen Miletic
Randall Bernard Mims
Raymond F. Minor
Ikenna M. Mmeje
Rebecca L. Morgan-Boyd
Melanie M. Nobello
Angelo Quaresima
Michael A. Reeves
Joseph Lee Roberson
Carlotta M. Rodriguez
Denise A. Roe
Ronald Philip Roemer
Johanna Stamates
Bethany A. Stanisiewski
Carla E. Wallace
Kathryn N. Wrench
Carrie L. Young
Taryn K. Zubich

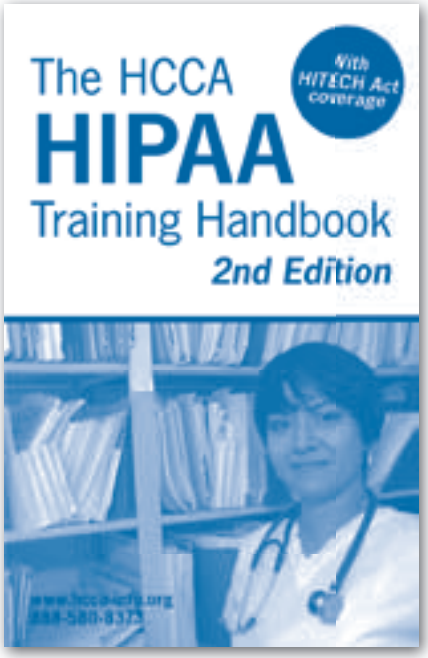
Congratulations!! The following individuals have recently successfully completed the CHPC® certification exam, earning their certification:

Jennifer Doherty Hurst
Kathleen Melo-Nazario
Carla E. Wallace

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

NOW AVAILABLE:

The HCCA HIPAA Training Handbook



The Health Insurance Portability and Accountability Act (HIPAA) has had lasting impact on U.S. health care providers since its passage in 1996. Now HIPAA, along with HITECH, affect health care professionals on a daily basis. This newly revised handbook is intended for anyone who needs a basic understanding of the privacy and security regulations governed by HIPAA and HITECH. Suitable for staff training courses, it covers:

- Who must comply with HIPAA and HITECH
- When and by whom is the use or disclosure of protected health information (PHI) permitted?
- What rights does an individual have regarding his or her PHI?
- What are the basic safeguards required to protect the security of e-PHI?
- What happens when a breach occurs?
- And much more

This handbook can prepare all health care professionals to help protect the privacy and security of their patients' health information.

Order Now

HCCA MEMBER DISCOUNTS

# of handbooks	cost per book
1–9	$25
10–24	$23
25–49	$20
50–74	$18
75–99	$16
100+	$15

THE HCCA HIPAA TRAINING HANDBOOK

Qty		Cost
_____	HCCA Members ($25 or see chart at left)	$ _____
_____	Non-Members ($30 per handbook)	$ _____
_____	Join HCCA!	$ _____
	Non-members, add $200 to join HCCA, and pay member prices for your order (regular dues $295/year)	

Total: $ _____

Bulk discounts available for HCCA members only. See chart at left to figure cost. All purchases receive free FedEx Ground shipping within continental U.S.

PLEASE TYPE OR PRINT

HCCA Member ID

First Name M.I. Last Name

Title

Organization

Street Address

City State Zip

Telephone

Fax

E-mail

Make check payable to HCCA and mail to:

HCCA, 6500 Barrie Road, Suite 250
Minneapolis, MN 55435

Or fax order to: 952-988-0146

☐ *My organization is tax exempt*

☐ Check enclosed

☐ Invoice me | Purchase Order # _____

☐ I authorize HCCA to charge my credit card (choose below):

○ AmericanExpress ○ Diners Club ○ MasterCard ○ Visa

Credit Card Account Number

Credit Card Expiration Date

Cardholder's Name

Cardholder's Signature

Federal Tax ID: 23-2882664

Prices subject to change without notice. HCCA is required to charge sales tax on purchases from Minnesota and Pennsylvania. Please calculate this in the cost of your order. The required sales tax in Pennsylvania is 7% and Minnesota is 6.5%.

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

6500 Barrie Road, Suite 250
Minneapolis, MN 55435
Phone 888-580-8373 | Fax 952-988-0146
www.hcca-info.org | helpteam@hcca-info.org

Letter from the CEO

Conflicts of interest

Preventing regulatory, policy, and ethical compliance problems is a complex proposition. However, we have a lot of people who want to make this more complicated than it is. Whenever I try to solve a complex problem, I look out the window. Well not exactly, but I do metaphorically speaking. Sometimes it helps to get away from all the noise. It helps to get away from all the "experts." Sometimes it helps to simplify a complex problem to find an easier solution. People tend to get lost in the weeds. They tend to overanalyze. They tend to complicate things. They want to show you how much they know. My brain can't handle too much information at once. I get confused. I get lost in the minutia. So I look out the window....so to speak.

I am going to try to simplify our rather complex and daunting job as the compliance and ethics professional. Our job is to prevent, find, and fix policy, regulatory, and ethical problems. What is it that is at the root of all intentional regulatory, policy, and ethical problems? I am not talking about mistakes here, just the problems that are known to exist but are not resolved, i.e. Enron, WorldCom, Tyco, HealthSouth, etc. The root cause is a conflict of interest. This in and of itself is not a profound revelation. However, I think the fact that we ignore the solution to the root cause (conflict of interest), for the most part, to be profound. I will get back to that in a minute.

Anyone who chooses to break a policy, behave unethically, or does not follow the rule of law has two choices: right and wrong. The only reason people choose to be wrong is because they will benefit in some way. They will gain more power, make more money, avoid bad press, etc. What they all have in common is that they are conflicted. If they were not conflicted they would not commit the foul in the first place or they would fix it the minute they became aware of it.

What bothers me is that we do a horrible job of identifying and dealing with conflicts of interest. Some don't think it's a big deal. Some people who are asked to complete a conflict-of-interest form are concerned about revealing or talking about their potential conflicts of interest. They think we are making too big a deal out of the potential conflicts. They don't see how their potential conflict of interest could cause a problem in the future. There are many reasons why we are where we are. Interestingly enough, the fix is quite easy. It just requires someone with a conflict-of-interest management procedure in their hands and a steel rod in their spine. Many have the procedure, but many cave when they are met with resistance.

Here is my point. If you agree that all intentional problems are caused by a conflict of interest, then life could be simpler for you. You can keep chasing the problems or you can go to the root cause and prevent them before they happen. For example, you could work with your organization to create incentives that override the monetary incentives. There are organizations that have made it a requirement to pass compliance and ethics program metrics before your bonuses, based on financial performance, kick in. Eliminating the financial bonuses is not realistic, but managing them is. Eliminating all conflicts of interest is impossible, but managing them better than we have is possible. There is a lot of work that can be done to align incentives in a way that causes people to do the right thing.

Of course it won't work every time, but you will be far better off spending time at the root cause than

Continued on page 22

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 Second Vice President of the HCCA Board of Directors. John may be contacted by e-mail at jfalcetano@uhseast.com.

You don't have to be quiet in this library

This month, I thought I would focus on the Library section of the HCCA Social Network site, which allows our members to exchange and share information. One way they do this is by uploading important documents to the social network libraries. This is one library where you don't have to be quiet when visiting. Libraries are a great place to obtain compliance documents to help further your compliance program. Below is a list of 20 documents that have been uploaded by your fellow compliance professionals:

1. Ten Things about Financial Statement Fraud
2. Accountability: The key to culture alignment
3. Accounting and Auditing: Related parties and related party transactions
4. An Ethics and Compliance Benchmarking Survey
5. Audit policy
6. Compliance Program Components - Survey Results
7. Compliance Programs
8. Compliance with State and Federal Data Breach Notification Laws
9. Compliance/Ethics programs: Risk assessments
10. Corporate Crime and Compliance: What does the government expect?
11. Director Training
12. Ethics and the Board
13. Exit Questionnaire with Compliance
14. Gift Policy Procedures and Samples
15. Guide to Conducting Workplace Investigations
16. Guide to the Sarbanes-Oxley Act: Internal Control reporting requirements
17. Helplines & Hotlines: What we know and can improve about reporting

Continued on page 22

Get Connected.

HCCAnet

Subscribe to dozens of discussion groups, download hundreds of resources, and connect with thousands of compliance professionals on HCCAnet
http://community.hcca-info.org

JOIN OUR GROUP LinkedIn

Start a discussion in the HCCA LinkedIn group
http://www.hcca-info.org/LinkedIn

FOLLOW US ON twitter

Follow @hcca_news for the latest trends in health care compliance
http://www.twitter.com/hcca_news

Find us on Facebook

Get the latest compliance news and HCCA event information in your facebook news feed. "Like" that HCCA facebook page at
http://www.hcca-info.org/Facebook

HCCA HEALTH CARE COMPLIANCE ASSOCIATION

Letter from the CEO

...continued from page 20

chasing problems down after the fact. If you identify the conflicts of interest, they can be managed or eliminated. Management of conflicts of interest is much simpler than you might think. It certainly is less painful than going through what Enron, WorldCom, and others went through. ■

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

Social Networking

...continued from page 21

18. Innovative Business Solutions: Improving the protection of health information
19. Internal Audit: The compliance officer's best friend
20. PCI – The Pathway to Compliance

As you can see, the libraries contain a wide variety of topics. Remember, social networking is a great way to make friends, obtain needed compliance documents, or just talk with peers. Visit our network, start a Blog, join a discussion group. You'll be glad you did. To participate in the discussion, review the comments, or just talk with your peers, you can access the Social Network site by going to the following link: www.hcca-info/hccanet. ■

Exhale

By Shawn DeGroot, CHC-F, CCEP, CHRC

Editor's note: Shawn DeGroot, CHC-F, CCEP, CHRC is Vice President of Corporate Responsibility at Regional Health located in Rapid City, South Dakota. Shawn also serves as Vice President of the HCCA Board of Directors. She may be contacted by e-mail at SDegroot1@regionalhealth.com.

Walk the talk

Frequently Asked Questions (FAQs) are a common method of providing quick answers or guidance on a common or specialized topic. FAQs also serve as a resource for quick answers without in-depth research. Guidance can also be derived from an organization's mission and values; essentially they serve as the foundation of any health care service, including the compliance program. The five core MERIT values that guide employees' work at Mission Health in Asheville, North Carolina are:

1. **M**ercy
2. **E**xcellence
3. **R**espect
4. **I**ntegrity
5. **T**rust/Teamwork

Jeri Williams, Vice President and Corporate Compliance Officer for Mission Health, has lived by those values and accepted the challenge of Internal Audit, Information Technology Audit, Clinical Audit, and Compliance Audit for more than 27 years.

What keeps Jeri up at night?

The abundance and ever changing list of rules and regulations. Jeri believes that the most critical requirement of her role as a compliance officer is to read, interpret, and apply the rules and regulations in a practical manner. First, to be aware that new rules have been proposed or issued means reading, planning, and preparing. The best method of obtaining the information and interpretations by other professionals is to subscribe to list-servs and numerous publications. Jeri's team subscribes to list-servs from HCCA, the Office of Inspector General (OIG), North Carolina Hospital Association, Palmetto GBA (Medicare Administrative Contractor), state Medicare and Medicaid work groups, the Association of Healthcare Internal Auditors (AHIA), publications from HCCA, and AISHealth's "Report on Medicare Compliance."

How does Jeri handle the stress of the role?

While system growth also increases her responsibilities, stress, and workload, Jeri enjoys the challenge of participating in the Mission Health System Services team. This is a team consisting of Information Technology, Finance,

Human Resources, Quality, Strategic Planning, Legal, Revenue Cycle, Audit, and Compliance that work together in an "on boarding" role with physician practices and member hospitals. Each area has a role and is assigned specific tasks to be accomplished. In addition to general compliance reviews, Jeri's staff perform initial coding reviews with the expectation that physicians will achieve a 95% coding accuracy rate. The audits and work are performed in a manner consistent with the Mission Health MERIT values, and Jeri finds the work invigorating by following a few key principles:

- **Invest in your team.** Team development is critical to achieve departmental and organizational goals effectively. Professional team development is important to ensure staff is furthering their professional skill set. Jeri leads her team by example, attaining continuing education from professional organizations as well. She strongly believes that if she is not on top of her game, she cannot expect her staff to be.
- **Stay organized and prepare.** Lack of preparation definitely adds a level of unnecessary stress. Disorganization leads to rework and inefficiencies.
- **Plan ahead.** Over her career, she has learned that planning upfront is a time saver. Anticipate questions or issues to avoid additional work.
- **Exercise is key.** Hiking, backpacking, or mountain biking are a few of Jeri's favorite activities that completely remove all thoughts from work in the exhilarating environment of the Western North Carolina mountains. Jeri works hard and takes time to play hard.

Jeri's advice to compliance officers is to focus on and develop data analytical resources. The increased regulatory audits necessitate that these resources be a key aspect of the Audit and Compliance leader's toolkit. Although it is easy to become frustrated and overwhelmed, maintain a perspective that a new regulation is simply a new challenge, and you have the opportunity to make a difference. If you don't enjoy challenges, then reflect on whether you are, or are not, in the right field. ■

Compliance Today Needs You!

Every month **Compliance Today** offers health care compliance professionals information on a wide-variety of enforcement, regulatory, legal, and compliance program development and management issues. To do this we need your help!

We are particularly interested in articles covering compliance concerns involving hospitals, outpatient services, behavioral health, rehab, physician practices, long-term care/homecare/hospice, ambulatory surgery centers, etc. For details, e-mail margaret.dragon@hcca-info.org with your topic ideas, format questions, etc.

Articles generally run between 1,000 and 2,500 words; this is a guide, not a limit. The title and the author's contact information must be included in the article. Articles should be submitted as a Word document with very limited formatting. Please select a deadline from the list below.

Upcoming Compliance Today Deadlines:

- December 7
- January 4
- February 1
- March 1

IMPORTANT: For those who are Certified in Healthcare Compliance (CHC©), please note that CCB awards 2 CEUs to authors of articles published in Compliance Today.


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 than page-turning text.

An effective training program requires more than 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

feature focus

Civil and criminal liability for overpayments

By Gabriel L. Imperato, Esq., CHC

Editor's note: Gabriel L. Imperato is the Managing Partner of the Fort Lauderdale office of Broad and Cassel. He is certified as a specialist in health law and is a member of the Board of Directors of the Health Care Compliance Association. He represents individuals and organizations accused of criminal or civil health care fraud and handles compliance matters for health care organizations. He may be contacted by telephone in Fort Lauderdale at 954/745-5233 or by e-mail at gimperato@broadandcassel.com.

The initiation of a federal health care investigation typically will involve a review by the enforcement authorities of potential criminal and civil liability. This is often, although not exclusively, the result of the filing of a private whistleblower action under the False Claims Act (FCA). Therefore, compliance professionals and legal counsel should be aware of not only the basis for criminal culpability, but also liability under the FCA. This potential exposure has now been the focus of recent Congressional action concerning what is commonly referred to as "overpayment liability." A recent amendment to the FCA has greatly elevated the risk to organizations for criminal and/or civil liability for the failure to promptly return "known overpayments."

There are a number of criminal statutes that can be invoked against health care providers, but a section of the Social Security Act (the Act) related to "overpayment liability" concerns false statements in connection with services paid for by a federal health care program. The Act imposes a duty to disclose and return known overpayments, requiring that

> whoever . . . having knowledge of the occurrence of any event affecting . . . his initial or continued right to benefit or payment . . . conceals or fails to disclose such an event with an intent to fraudulently secure such benefit or payment [shall be subject to criminal penalties and fines].[1]

These penalties include a fine of not more than $25,000 or imprisonment of not more than five years, or both. This particular statute has historically been referenced by enforcement authorities as a basis for criminal culpability for failure to "return a known overpayment." However, enforcement actions under this statute have been sparse, and there has always been some lingering uncertainty surrounding the existence of a specific duty to self-report and refund overpayments by virtue of this statute.

False Claims Act liability

The FCA imposes basic liability for knowingly submitting or causing the submission of a false or fraudulent claim. However, an additional basis of FCA liability for a failure to return an overpayment previously required someone to actively use a false statement to conceal, avoid, or decrease an obligation to repay the government. In the past, the FCA punished these "reverse false claims" where the actor: knowingly ma[de], use[d], or cause[d] to be made or

used, a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the Government.[2]

Under this prior, fairly narrow, provision, a party needed to do more than merely avoid repaying the government. To be culpable, the party had to take the affirmative step of making or using a false record or statement for the purpose of avoiding repayment. Thus, there was no true legal obligation under the FCA to self-report overpayments.

The recent amendments to the FCA have dramatically changed, and ultimately increased, liability for overpayments. In May of 2009, the Fraud Enforcement and Recovery Act of 2009 (FERA) made significant changes to the FCA, including an amendment to the reverse false claims provision. Under the amended provision, codified at 31 U.S.C. § 3729(a)(1)(G), liability is imposed on anyone who:

> knowingly makes, uses, or causes to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government.

This provision applies to both (1) taking the affirmative action of using or causing to be used a false record or statement to avoid having to pay money to the government; and (2) affirmatively hiding the existence of funds, or improperly avoiding an obligation to pay the funds to the government. As a result of FERA, an individual is potentially liable under the FCA for failing to refund money it is obligated to pay to the government, even if these funds were obtained or retained without a "false record or statement." FERA defines an "obligation" as "an established duty, whether or not fixed, arising from an express or implied contractual, grantor-grantee, or licensor-licensee relationship, from a fee-based or similar relationship, from statute or regulation, or from the retention of any overpayment."[3]

This means the provisions of the FCA now cover a health care provider's retention of overpayments regardless of whether the provider ever makes a false statement to conceal the overpayment or even submits or presents a claim for payment.

Affordable Care Act amendments

Furthermore, FERA's definition of the term "obligation" initially created some confusion over whether the retention of an overpayment would in fact be considered an obligation under the statute. The Patient Protection and Affordable Care Act (PPACA), signed into law on March 23, 2010, offered some clarity on the issue. Section 6402 of PPACA is entitled "Enhanced Medicare and Medicaid Program Integrity Provisions" and provides that all overpayments must be reported in writing, along with an explanation for the overpayment, and refunded within 60 days of the date such overpayments are identified. The term "overpayment" is explicitly defined as "any funds that a person receives or retains . . . to which the person, after applicable reconciliation, is not entitled."[4]

PPACA clarifies that a repayment retained after the deadline from "identification" for reporting and repaying it is indeed an obligation under the FCA. Thus, a health care provider who fails to report and return overpayments within 60 days of "identification" potentially faces liability under the FCA. A whistleblower can now file a complaint under the FCA, based on the mere allegation that an organization "failed to return a known overpayment." Additionally, a determination that an individual knowingly concealed overpayments from federal health care programs may be grounds for criminal penalties.

Continued on page 28

 ...continued from page 27

Criminal liability aside, FCA violations may result in multiples of damages and/or monetary penalties of $5,500 to $11,000 per claim and/or exclusion from federal health programs. Section 6402(d) of PPACA also amends the Civil Monetary Penalty statute, which may be invoked directly and independently by the Department of Health and Human Services (HHS) Office of Inspector General to establish civil monetary penalties for failure to report and return known overpayments. There are regulations pending by HHS to clarify an organization's obligation and the timeline for reporting overpayments under these administrative authorities, which may be published before the end of the year.

Conclusion

FERA and the PPACA have dramatically expanded the scope of exposure for health care providers under the FCA. These recent amendments make it clear that a health care provider has an affirmative duty to return an overpayment to the government and it may be that these provisions apply to overpayments received prior to their effective date. Providers should work quickly to minimize liability under the new provisions by reviewing existing compliance programs to ensure that procedures for reporting and refunding overpayments satisfy the requirements of the law and "best practices" for an effective compliance program. ■

The author would like to acknowledge and thank Danielle Viera, a law clerk with Broad and Cassel, for her assistance in the preparation of this article.

1. 42 U.S.C. § 1320a-7(b)(a)(3).
2. Previously codified at 31 U.S.C. § 3729(a)(7).
3. 31 U.S.C. § 3729(b)(3)
4. Patient Protection and Affordable Care Act, Pub. L No. 111-148, 124 Stat. 119 (2010).

They will never remember the vendor; you, however, are unforgettable…

By: Laurie Smaldon and Gretchen Hood

Editor's note: Laurie Smaldon is a Director with PwC Health Industries. She may be contacted in Hartford, Connecticut at 860/241-7011 or by e-mail at laurie.a.smaldon@us.pwc.com.

Gretchen Hood is Manager, Privacy & Security Enterprise Vendor Management, with Aetna Life Insurance Co. and may be contacted by e-mail at hoodgg@aetna.com.

Vendor management is a whole new world. In the not-so-distant past, when entering into a contractual agreement with a third-party vendor, the biggest concern was likely fees and assurances that the service contracted for would be provided on time. Today, however, the stakes are significantly higher; in particular, ensuring that whatever third-party vendor you entrust your organization's data with will keep it as secure as you would. Although business associate agreements and indemnity clauses can provide some level of contractual assurance, is it enough? Will your patients, members, or customer base accept as a reasonable explanation, "We had a contract in place. What more could we do?" With a high percentage of breaches involving errors or data compromised while in the possession of a third party, it is too big a risk to ignore. Aside from the monetary fines and penalties that often come with a data breach, there is the potential reputational damage—damage to brand and loss of consumer confidence—those indirect ramifications of a breach can be costly. If a consumer does not trust or believe their provider or payer organization has the appropriate privacy and security controls in place, it is almost evitable that they will move their business to another organization, adversely affecting the bottom line.

Added to this is the inevitable press coverage which could be highly visible (especially if your organization is well known and easily recognizable), and the number of new laws and regulations that specifically address vendors and contractors. The Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act upped the ante with regard to business associates. What was once a contractual obligation is now a regulatory requirement for business associates. The federal breach notification provisions require reporting unprotected data breaches of more than 500 records to the media and the government which, in turn, will post the loss on its website.[1] Other laws that lead the pack in specific requirements for vendors are the Massachusetts Standards for the Protection of Personal Information (201 CMR 17.00) and the Payment Credit Industry (PCI) data security standards.

So what's an organization to do? With the increase in outsourcing (and in some instances, the globalization of outsourcing), the reality is the need to work with vendors and suppliers and assure a level of confidence that the data you've shared or provided to them is adequately protected. How to secure those assurances beyond the contractual agreement is the question and the challenge. In response, leading organizations are now proactively and aggressively managing their vendor relations, whether that is through an annual attestation, on-site audits, or self-reporting. There is now, more commonly than not, a requirement that specific controls (beyond contractual requirements) be in place to

Continued on page 30

 ...continued from page 29

ensure that the organization and the member/patient can breathe a little easier with third-party access and use of their data.

Key points to remember:

- Many new laws in the U.S. and globally increased regulatory oversight and enforcements
- Highly visible press coverage of identity theft and data breaches
- Increase in outsourcing and, in many instances, global outsourcing.

Pre-contract process

Leading practice organizations are now enhancing and designing their pre-contract process to be a thorough assessment of the vendor. This includes reviews of privacy and security controls prior to actively engaging for services and certainly before releasing member or patient non-public information (NPI), protected health information (PHI), or personally identifiable information (PII) for processing. With the cost of a breach caused by a third party rising significantly per record, and increased regulatory scrutiny and press coverage, the benefits of pre-contract diligence generally offset any changes to operations required to conduct the assessment and evaluate the risk.

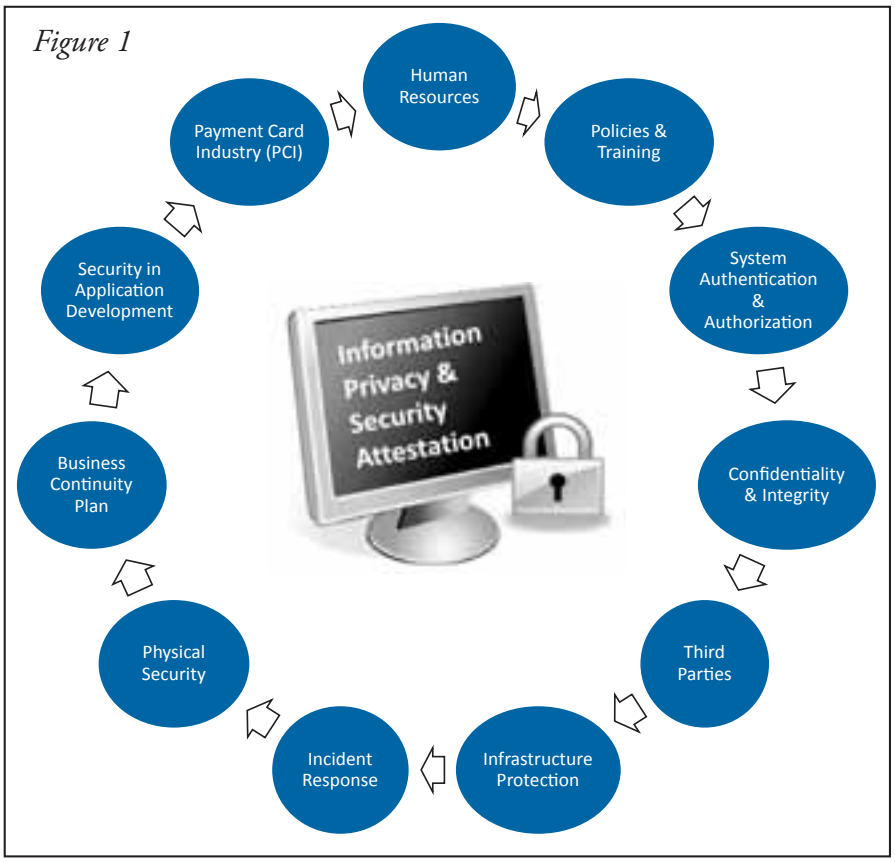
As part of Aetna's vendor pre-contract assessment, a series of administrative, physical, and technical requirements have been identified to improve the vendor's ability to adequately protect from theft or data breach the member data entrusted to them.

As part of the due diligence in the pre-contract phase, and before a contract can be signed, the vendor is risk-stratified. The risk-stratification process takes into account a number of factors in assessing the overall risk of the supplier based on the following criteria:

- Services provided
- Method of access, receipt, and/or storage of confidential non-public member or employee data
- Type and volume of confidential non-public member or employee confidential data
- Impacted member/employee base

Depending on the risk-stratification outcome, the vendor is required to complete a privacy and security attestation to attest to its compliance with a series of controls and requirements. New vendors have one to two weeks to complete the attestation. Upon submission of the completed attestation, internal cross-functional subject matter specialist(s), representing business units such as IT, Human Resources, Physical Security, Compliance, and Privacy, review the attestation responses and any supporting documentation to determine the vendor's compliance. If the vendor is accepted and engaged to conduct services for or on behalf of Aetna, it is now in Procurement's

Figure 1



line-of-site and integrated into the annual assessment process. (figure 1)

Key points to remember:

- Risk-stratify vendors, based on regulatory and business criteria, to prioritize ongoing monitoring.
- Adjustments to operations to incorporate due diligence in the pre-contract phase will far outweigh the cost or negative publicity of a vendor breach.
- Business units and subject matter specialists should assess controls and vendor responses beyond regulatory frameworks.

Privacy and security attestation

The privacy and security attestation, used in the pre-contract due diligence phase (and annually thereafter) is a proprietary tool built by Aetna, based on HIPAA, HITECH, International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST) and the Electronic Healthcare Network Accreditation Commission (EHNAC) standards. Unable to identify a single industry certification that met all of Aetna's specifications and requirements, the company developed its own, which includes input from its business operations and subject-matter specialists on privacy and security controls. The certification pinpoints the most critical business requirements.

The privacy and security attestation tool measures a vendor's compliance with 11 category controls (see Table 1 below).

These 11 control areas address 75 specific requirements. A vendor can be "compliant," "compliant with mitigating controls," "non-compliant," or "partially compliant." Compliant with mitigating controls requires the subject-matter expert teams and Procurement to gauge how acceptable the mitigating control is for the level of risk that Aetna is willing to tolerate.

Key points to remember:

- Attestations should be comprehensive and broad-based, including business needs or requirements in addition to regulatory frameworks.

Continued on page 32

Section	**Requirement Example** *Table 1*
Human Resources	■ Criminal background checks prior to date of hire
Policies & Training	■ Formal documented privacy and security policies and procedures ■ Evidence of policies reviewed at least annually ■ Process to annually obtain employees' attestation to agree to abide by all policies.
System Authentication and Authorization	■ Password Complexity ■ Role based access rights
Confidentiality & Integrity	■ Encryption on ALL physical media
Third Parties	■ Disclosure of all third parties and services with direct or indirect access to Aetna data
Infrastructure Protection	■ Antivirus Software ■ External vulnerability assessments
Incident Response	■ Information Security incident response plan
Physical Security	■ Physical security and access control measures
Business Continuity Plan	■ Formal BCP plan including testing and pandemic readiness plan
Security in Application Development	■ Industry standard requirement in controls in application development
Payment Card Industry (PCI)	■ PCI/DSS compliance

- There are circumstances where "compliant with mitigating controls" can be an acceptable level of risk; the evaluation of a vendor's security and privacy posture is not necessarily black and white.
- Ongoing monitoring and annual recertification ensures ongoing compliance with privacy and security requirements
- Contractual provisions which link to the privacy and security oversight processes and requirements further ensure a legal obligation and protection for vendors to remain compliant.

Annual assessment process and on-site assessments

On an annual basis, 20 to 25 vendors (or 10% of the supplier base) are selected for an on-site assessment conducted by an independent, objective third party. Vendors are selected based on risk, including such key indicators as services provided, transaction volume, geographic allocation, spending, etc. Other criteria considered include past performance (e.g., a breach during the previous year) or the anticipation or expectation to conduct significantly more business with a vendor in the coming year.

Repeat assessments are also possible, but not random. A repeat assessment could be a result of poor performance on a prior year on-site assessment or concern with how an attestation was completed/responded to. Attestations that are poorly responded to, or appear to be "check-the-box" with little thought or commentary, are almost certain to be flagged for an on-site assessment.

On-site assessments are limited to the scope of the attestation. Assessments include interviews, document review, and limited testing. The assessors will take into account SAS70 type II2 assessments that the vendor may already have conducted, but in general, SAS70s usually do not include privacy and security controls or the level of depth or scrutiny to assure data is adequately protected. The primary purpose of the on-site assessment is to validate operations ensuring that controls are in place and functioning as attested to. The outcome of the on-site assessment is a detailed matrix based on its 11 domains in the attestation with a determination of the vendors' compliance. The report substantiates the findings.

To the extent practical, at the time of the on-site assessment, remediation and time frames for remediation are agreed to and documented with the vendor. The vendor receives a copy of the final report as does the business area(s) that contract with the supplier. The vendor has three weeks to provide a management gap analysis and action plan, which includes its intent to remediate within specific time frames or dispute the finding. Non-compliance must be remediated, and timelines for remediation must be agreed upon and approved. If the on-site findings show an overly abundant number of controls resulting in a non-compliant finding or sheer dishonesty in responding to the attestation, this can result in an immediate exit strategy and putting the business back out to bid. Vendor relationships have been terminated based on on-site assessment findings. Poor performance, let alone material breach, can have significant adverse consequences, above and beyond regulatory fines and penalties, including irreparable damage to brand and reputation. The decision to exit a relationship with a vendor must result in a collaboration among the business unit, Procurement, and Legal. This may include when necessary, identifying a new supplier and/or initiating an exit strategy.

At the conclusion of all on-site assessments for the year, an aggregate view is compiled and shared with the customer population or plan sponsors. What was once an infrequent request for performance measures by plan sponsors is now common. From a management perspective, the request for performance is proactively

Continued on page 33

identified, including the assessment of trends and weaknesses, so that remediation can be implemented in a timely fashion. At Aetna, having a contract in place is far from all we can do to ensure the privacy and security of outsourced data.

Key points to remember:

- Third-party on-site assessments substantiate and validate vendor assurance provided in annual attestations.
- Be prepared to exit relationships or have an exit strategy when controls are materially non-compliant or the time to remediate presents a level of risk that is unacceptable to the business.
- Consumers, patients, members, and plan sponsors will increasingly demand evidence of proper controls in protecting their non-public information (NPI), protected health information (PHI) or personally identifiable information (PII).

Conclusion

Outsourcing data to third-party vendors is a good business strategy. Outsourcing often provides a means to offer additional services or lower costs of services to members and patients. The risk, however, of providing member or patient PII or PHI to a third party and ensuring adequate controls and protections cannot be dismissed. It is not enough to rely solely on contractual provisions to ensure an adequate level of data protection. Pre-contract due diligence, annual attestations, and on-site assessments all involve a level of effort, cost, and additional steps, but the benefit of securing additional assurances (and testing those in some cases) far outweighs the cost and negative impact of a data breach. They will never remember the vendor that had the data breach; you and your brand, however, are unforgettable. ■

1. Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/postedbreaches.html
2. For more information on SAS, see http://sas70.com/

Discover the antidote to data breach strain.

Finding the resources to clean up a data breach causes stress for you, strain on your staff, and slows down your whole organization. But it doesn't have to be that way.

More health care organizations trust ID Experts® as their partner for data breach solutions than any other vendor. We work with you to eliminate the strain of data breach by supplementing your team with our expertise and substantial resources.

Only ID Experts has proprietary tools for assessing the unique compliance requirements surrounding loss of PHI. We tailor each breach response to address the real risks to your patients — and your reputation.

Through November, **request a free trial** of our data breach recovery solutions for use on your next breach of fewer than 500 records*. Act now to see for yourself why ID Experts is the antidote to data breach strain.

Experience a less painful recovery from data breach.

Visit www.TryTheAntidote.com today.

Request a **Free Trial** of ID Experts® breach recovery solutions

idexperts®

* New clients only. Visit www.TryTheAntidote.com for complete offer details.

HAVE A BREACH NOW? Call our Data Breach Lifeline: 866-726-4271

Joshua's Law: Patient privacy

By Christopher R. Gingras, FACHE, FHFMA, CHE

Editor's note: Christopher R. Gingras is Vice President Healthcare Compliance with Musculoskeletal Clinical Regulatory Advisers, LLC (MCRA) located in Manchester, Connecticut. He may be contacted by telephone at 860/904-4451 or by e-mail at cgingras@mcra.com.

On June 2, 2009, a New London, Connecticut police officer was dispatched for a reported drug overdose. Upon arrival at the local Red Roof Inn, he took two photographs with his cell phone camera of the deceased patient. These photographs were distributed electronically to his fiancé and three of his friends. One of the individuals who received the photograph recognized the patient and contacted the New London Police Department to report this incident.

In response to this incident, Connecticut recently passed a law prohibiting first responders from taking photographs at crime or accident scenes and transmitting them to private individuals. This law has become known as Joshua's Law, in reference to the overdose victim, Joshua Rogers, a Connecticut National Guardsman.[1]

In reading this story and many others like it, I am bothered on different levels. As a Connecticut fire fighter and first responder, it is an embarrassment to me as a professional that an individual would exercise such poor judgment and violate the trust our patients place in us when they call 911 for help. Irrespective of the circumstance or manner of death, each patient deserves respect and proper care. They are not to be derided on Facebook or have their photo e-mailed with the tag line "This is what happens when you overdose."

Unfortunately, stories like this can be found throughout the country; whether it is in an ambulance first on scene or a health care facility Emergency Room (ER), these photos have been posted on Facebook, sent in Tweets, distributed by e-mail, or found on a misplaced iPhone. One only need ask former US Representative Anthony Wiener (Dem–NY) about the reputational damage that can result from the distribution of a photo through Twitter.

The question and challenge for us as compliance officers is how do we best educate our employees and other organizational representatives to conduct themselves in a professional manner consistent with our robust patient privacy policies? How do compliance or privacy officers make this real so that employees understand the significant violation of patient trust that occurs and the risk that they put themselves in, both personally and professionally? In addition, there is significant risk to the organization, because we are now seeing more and more fines and investigations related to privacy breaches.

In this article I hope to use this recent example, the newly enacted Connecticut law, and the subsequent discipline taken against this police officer to provide some valuable lessons that might be helpful in formulating a three-step risk mitigation strategy.

Step 1: Policy and procedure

The first step is to ensure that a written policy exists in regard to the appropriate and inappropriate use of clinical photographs or videos within your organization. The use of photographs in the provision of clinical care is not new. What is new is the quality and size of cameras that are ubiquitous with worldwide distribution a click away. To the benefit of patient care, the use of cameras and video recording has become more integral, whether for tracking a skin rash, video recording patient answers in an assessment, or the dozens of apps that help physicians

Continued on page 36

 ...continued from page 35

resolve complex clinical events. As an example, a recent ad for the iPad shows it being used during an ambulance transport to teleconference with the receiving hospital. This is a fantastic use of technology that we would do not want to impede in our efforts to protect our patients from privacy breaches.

Policy development considerations

Convene a multi-disciplinary team involving nurses, physicians, ER management, and information technology on your policy development or review team, and consider the following:

- Does the policy clearly state that a patient photo cannot be taken unless it is clinically appropriate?
- Do you require written or verbal patient consent? How do you document verbal consent? Your Notice of Privacy Practices, General Consent, and Surgical Consent should all include references to the clinical use of photographs within the institution.
- Have you completed an inventory of clinical areas that take photographs? The ER, wound care, and plastic surgery are the usual suspects. Are there more?
- Have you completed an inventory of the types of devices that exist within your organization? Do you have enough easily accessible, quality cameras to meet the clinical needs?
- Can a personal device, such as an iPhone, be used to take clinical photographs? If yes, do you have a policy to mandate protections on the personal device, such as encryption, remote delete, and password protection? Do you have a smartphone policy?
- How do you handle members of the medical staff that are not employees, who may not have an organizational device issued to them, and may not have an organizational encrypted e-mail?
- How do you protect, track, delete, destroy, and encrypt the memory cards contained within a department camera?
- How do these photos migrate from the device to the electronic medical record? Do you have a way to store clinical photos in the electronic medical record (EMR)? If not, how do you make these photos available?
- Do you know where photographs are currently stored? Are they located on a server or a surgeon's desktop? Many organizations only encrypt laptops. This puts patient data, such as photographs on a desktop computer, at greater risk. In addition, they are probably not being properly backed up.
- Is this policy integrated into your existing social media and information security policies?

There are lots of issues to consider when developing a policy, but the most important and the one that seems most evident is that patient photos are only taken when medically necessary and *never* shared with anyone not directly involved in the care of the patient.

Step 2: Education

Once the policy has been written or revised, we want to communicate to our employees the expectations of behavior in relation to this very important topic. When developing education or training, my recommendation would be to make it SMART:

- **Simple:** We have all heard the saying: Keep It Simple Stupid." The policy might be a few pages long, but we need to simply state that the purpose of the policy is to provide direction on the appropriate and inappropriate uses of patient photographs. In the fast paced health care work environment, employees do not have the time to read lengthy paragraphs or navigate a treatise on patient privacy. Make your communication catchy, interesting, and possibly fun.
- **Measurable:** Can you demonstrate that an employee took the training or is aware of the policy? Can you demonstrate that the employee understood the material being presented? When disciplining or terminating an employee, we need to show that the employee was aware of or knew that his/her actions were improper. A simple

employee acknowledgement and a short assessment would be sufficient.

- **Actions:** What do we need the employees to do? This might involve conducting an inventory of devices or clinical uses of photography in their area, or simply be aware of where to find the policy if questions arise. We also want to make them aware of the Compliance Office and Compliance hotline in the event they become aware of improper behavior.
- **Relevant:** Why should an employee care? Discuss the consequences for them, which may include discipline, loss of job, loss of professional license, or the opportunity to make new friends in prison. Discuss the painful consequences for the patient or family who have now had their trust violated. Provide real world examples found in the news or even events which may have occurred within the institution. Ultimately we want our employees to act in a manner consistent with being a compassionate health care provider.
- **Timely:** The training needs to be frequent and timely. The training on this topic, and patient privacy in general, should occur as frequently as possible. This would include annual web-based training, posters, e-mail reminders, and materials posted prominently on the organizations Intranet site. We can never provide too much compliance and patient privacy training.

Step 3: Discipline

An element of an effective compliance program is that an individual needs to be held accountable for their actions and appropriately disciplined. In my professional experience, an employee e-mailing inappropriate photographs of a patient would be immediately terminated. In this specific case, the police officer was terminated but reinstated seventeen months later, after the union successfully argued that he was fired without "just case." The standard of just cause can be boiled down to seven tests: (1) Adequate warning; (2) Reasonableness; (3) Completeness of investigation; (4) Objectivity of investigation; (5) Proof of infraction; (6) Rules applied fairly; and (7) Punishment fit the crime.

A failure of one of these elements can result in the discipline being overturned, and probably the most significant in this case was the lack of a clear policy or education provided to the police officer that such conduct was inappropriate and could result in termination.

Whether your organization is unionized or not, I think we can all learn from this case the importance of clearly articulating the standards of behavior expected of employees and the disciplinary actions that may result when those standards are not followed. It is imperative to conduct annual training and have a code of conduct and robust policies, so that when disciplinary action is taken, the action will be upheld through any level of appeals that an employee may pursue, either internal or external.

As a compliance or privacy officer I want to have no doubt that each and every employee in my organization is aware of the clinical photograph policy and related patient privacy policies. My hope is that the next time an interesting case presents in the ER, an employee will exercise good judgment and not choose to place a photo on Facebook. We owe it to our patients and to the community we serve to treat them in a manner no different than what we would expect if the roles were reversed. ■

1. JC Reindle: House OKs 'Joshua's Law.' The Day, May 26, 2011. Available at http://www.theday.com/article/20110526/NWS12/305269373

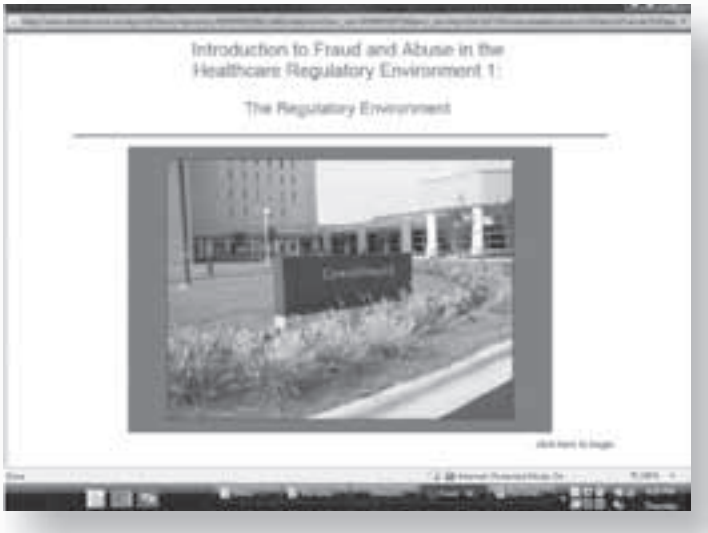
Let's you and I talk about effective Healthcare Corporate & HIPAA compliance training for your staff, contractors, and physicians

Healthcare facilities that are serious about training and educating their staff choose eHealthcareIT and PricewaterhouseCoopers.

We don't need to tell you, healthcare compliance is a very serious business. In fact, one of the greatest risks to consider in 2011 is the increase in targeted healthcare fraud enforcement efforts by the government's Health Care Fraud Prevention and Enforcement Action Team (HEAT).

Expertise

PricewaterhouseCoopers' Health Industries Practice and eHealthcareIT is comprised of highly qualified healthcare professionals specializing in regulatory compliance. Included within this group of professionals are physicians, registered nurses, certified coding specialists, registered records administrators, certified public accountants and attorneys.



Engaging & Practical Learning

Reliable, engaging, IT friendly and up to date content is key to a successful compliance education program, which is what eHealthcareIT brings to the table.

You know as well as we do that one size does not fit all:

- Over 100 engaging, department specific HIPAA Compliance, Clinical Research Compliance, and Corporate Compliance courses.
- Customization that allow you to embed your policies, procedures, welcome messages, site specific pictures and "contact information".
- Department specific topics ensures that your staff will receive compliance education geared specifically to their needs and responsibilities.

Your compliance education should not be a matinee at the movies. Contact eHealthcareIT for further information or consultation.

eHealthcareIT
eLearning & IT Solutions

email: info@ehealthcareit.com
or call 1-800-806-0874.
www.ehealthcareit.com

Review of compliance fundamentals

By Alexandra F. Holt, CHC

Editor's note: Alexandra F. Holt is the Chief Compliance Officer and Chief Privacy Officer for HMS in New York City. She chairs the Internal Corporate Compliance and Security Committees and directs the corporate compliance program for all HMS operating entities. In addition, Alexandra is responsible for policy development and implementation, compliance training and communications, auditing, and issue reporting and resolution. Alexandra may be contacted by telephone at 212-857-5337or by e-mail at aholt@hms.com.

You have been asked to become Chief Compliance Officer. You are going to take over an existing program or start a new one. Now is a good time to review fundamentals and clear your head before the rush of To Do's takes over. Others will have ideas about what you should do, but in order to lead effectively and stay focused, it helps to review the challenge relative to some first principles.

Ethics and values

As compliance officers, we are called to embody and uphold a set of ethical standards, communicate them clearly, and exhort others with all of our powers of persuasion to adopt and support them too, while they are employed by or affiliated with our organization. We are asked to create "an ethical culture" wherein everyone "lives the core values of the organization." That's a tall order. What does it really mean? Let's analyze and revisit key underpinnings of successful, effective compliance programs.

Ethics

The dictionary defines ethics as the set of "obligations and duties a society requires of its members." Among the obligations and duties required by society are that we be law-abiding citizens. Thus, at a minimum, adherence to law is at the foundation of ethical culture. What this means is that pertinent laws should drive the initial structure of your organization's compliance program, and adherence to that law (as embodied in program policies) should be a corporate value. Is adherence to and respect for law stated in your organization's values? If not, put that in place as a first principle. My point may seem so basic as to be simplistic, but there have been heavy fines meted out to organizations that failed to adhere to this fundamental axiom.

People damage an organization and themselves for the simple fact of not obeying the law. You read about them every day, so the message bears repeating. Obeying and respecting law should be the first obligation you require of your corporate citizens and business affiliates.

Values

Next, step back and cast an eye on values your organization has already articulated or espoused. This exercise will give you some insights, so let's take a look at a few.

- **Respect for the patient.** In other words, we honor a patient's human dignity and his/her right to privacy of information. All good.
- **Integrity.** In other words, here at Organization X our word is our bond. We do not cut corners or promise what we do not intend to deliver. We are fair in our dealings and do not lie, cheat, or steal. Excellent.

Now step out into your organization and listen and watch. See if these and other value statements are evident in observed behavior. If not—if it's considered okay to put prescription information unshredded into the trash, if it's "Oh, that's just marketing" to misrepresent a benefit and its cost, if a certain doctor is getting preferential treatment behind the scenes for referrals, if people say

Continued on page 40

 ...continued from page 39

"Uh oh…here comes Compliance"—you have what is euphemistically called a cultural problem. But, said plainly, you have an ethical problem. What you are seeing and hearing in behavior is, in some cases, disregard for law and in other cases, a cynical sense that it's all right to spout nice phrases, but there is a hidden set of rules for certain members of this mini-society.

If you witness these discrepancies between what is said and what is done, you can be sure your organization has adopted them as acceptable behavior on some level, and you are now faced with a choice. You can stay and fight for change—which means defining and demanding ethical behavior for this organization—or you can request another assignment. This assessment is vital and requires honesty and courage. It is clear from legal history that having a half-baked compliance program (i.e., one that looks great on paper, but one more people don't live by than do) is the worst of situations. You will be held responsible for the actions of others, who sooner or later will engage in behavior that will put both you and the organization at significant risk. So, think carefully about the ethical and behavioral challenges your organization might pose, and whether you can overcome them and create a great compliance program.

You would like to see a basic commitment to law-abiding behavior up and down the line. It's important to accept that no organization is perfect, but neither should we lead an anemic endeavor. Reflect on Enron—a case where a compliance program and a 64-page Code of Ethics proved to be a sham, because abiding by law was neither a required nor endorsed behavior.

If your answer is "Yes, I accept this challenge," then start by stating your organization's values, policies, and procedures in accordance with law and commanding behavioral alignment with law. Then, design your program so that it includes basic compliance program elements, as stated by the Department of Justice (DOJ), and further articulated in the Federal Sentencing Guidelines (FSG). This will ensure that your program contains all the components deemed important by lawmakers and enforcement agencies—the ultimate arbiters of the effectiveness of your program.

On to the next principle. It is essential to have engaged and direct support from an ethical CEO and board.

Governance

Following the guidance set forth by the DOJ and the FSG, and to the extent possible given the size of your organization, ensure your position is structured so that you:

- are full-time; Compliance is not a trivial undertaking, nor do you want to have internal or external conflicts of interest;
- are an independent, valued executive reporting to the position of power in your organization and your agenda is visible to and supported from the top; and
- personally make reports to the Audit or Compliance Committee of your board of directors without interference from others.

Not only do the recently updated FSG re-emphasize this governance structure for an effective compliance program, it makes common sense. The board is ultimately responsible for the compliance program. They have a duty of care to perform with regard to the activities of the organization. It takes a three-part team (board, CEO and compliance officer) to have the best chance of creating a vibrant, ethical, and powerful compliance culture. If the FSG-recommended structure meets with resistance in your organization, there must be an alternative that meets an equivalent standard of accountability for the board and the CEO. If that's not extant, you are probably fighting an uphill battle to create an effective program. Leadership must acknowledge and stand behind the

ethics and values they purport to espouse and the duties they have signed up to perform.

Within the program structure, you should have the power to request resources as appropriate, as well as to establish a process that rewards compliance and punishes non-compliant behavior. The latter is fundamental, because it's common that managers argue for retaining those who have violated policy or ethical principles "because they are otherwise good performers." Without a clear corporate mandate that those who violate ethics and policies incur a genuine risk of termination (be they executives, employees, or business partners) through equitable processes applied to all, the program will devolve to a paper tiger. Work closely with Human Resources (HR) and executive management to ensure that adherence to compliance values and policy are part of all performance appraisals, compensation, promotion, contracting, and financial decisions. Set standards and processes for termination of a relationship; act on the standards and use the processes. Likewise, have reward programs—with significant remuneration and recognition—for those who contribute improved processes, creative ideas, and/or embody the principles of ethical behavior. Your program's power to affect behavior, sponsored by corporate leadership, is vitally important to regulatory authorities who evaluate the effectiveness of compliance programs and audit for "tone from the top." Structure a compliance program that puts its money where its mouth is.

Partnerships—compliance is everybody's business

Close working relationships, ones in which you can pick up the phone to obtain detailed information or adapt a process, contribute to a robust compliance program. In health care compliance, we should have these types of relationships with Security and Facilities, HR, Quality, Risk Management, Finance, Research, Contracts and Legal, and possibly other departments. It is not humanly possible for the compliance officer alone to stay on top of all that compliance entails. We need others' input, experience, data, and creative support to make sure the organization is the best it can be. Make individuals within your organization your partners—encourage them to ask questions, bring forward their ideas, and tell you their concerns. Enlist them as volunteers to oversee improvements and reward them for their efforts.

A hotline is great, and often mandated, but information given directly to you in the form of a question or concern is pure gold. Personally make the time to listen and be available for counseling—it's training in disguise, and it builds respect. On that topic, train with questions and case studies. This method not only confirms learning, it makes people come up with an answer together and with you. They will internalize a message of accountability, and they are more likely to partner with you as a result. In return, you will keep learning about your evolving business and have your finger on its pulse. So ask yourself: Who are your partners now as you take up your role, and how can they help you?

The power of the question

Compliance often entails exercising judgment in grey areas. It also requires the power to challenge the status quo if required. The question is your tool to gather information or mount a challenge to undesirable activity. Ask questions and follow up with more. Keep probing. By asking multiple questions of many people, you not only better everyone's chances of acting on reliable and complete information, you also set an example. If your organization is not in the habit of asking questions to further insight or clarity, make it a corporate value to do so. A culture which responsibly questions is one that will drive towards improvement over time. "Why?" is perhaps the most powerful question of all.

Continued on page 42

 ...continued from page 41

Do people ask questions in your organization? Do they fear retaliation if they do? Give corrective feedback to those you observe behaving in a threatening or shaming manner toward someone asking a question or raising a concern. Make sure the message of non-retaliation is loud and clear for anyone bringing a bona fide question or issue to the table.

Metrics and patterns

Do you have the process necessary to capture compliance metrics? As compliance officers, we have a responsibility to prevent and detect issues, as well as remediate problems, and what we can't measure we can't improve. We need to determine what our Compliance "Key Performance Indicators" are, and then track trends. Count errors per million, violations by type, improvements made by individuals or groups, training not completed or skipped, terminations for compliance reasons, compliance score by department, number of coding errors, outstanding achievements, contracts inappropriately executed, bank deposits gone awry, computers stolen, PHI not encrypted—whatever is meaningful to your organization, its values and its quality aspirations. You will need to enlist help from others to do this. In so doing, discipline yourself and your organization to the naming and remediating of the root cause of errors reported and counted, as well as successes achieved. "Lessons Learned" sessions also consolidate progress, and involve everyone in a memorable and positive way.

Metrics and trends, kept carefully over time, are powerful allies. First, they demonstrate oversight and assessment of the compliance program and can show meaningful systemic improvements being realized. Second, you and others can spot red flags in the data and chart courses of action efficiently, even preemptively. Third, you will have evidence to support any disciplinary or reward action required. Fourth, you can compare the effectiveness of your program to internal and external standards. You will have a meaningful context within which to report to the board.

Finally, urge your organization to a Six Sigma standard of excellence. It's difficult to achieve, but it demonstrates commitment to a high and widely recognized standard. Once attained, it is a source of real pride to the organization. A 1% error rate (99% quality rate) is 10,000 errors per million; Six Sigma standard is 3.4 errors per million. Why would we be satisfied with 10,000 errors per million? Where would you start measuring against this standard?

Responsiveness

Because Compliance cannot preemptively control everything, being responsive—acting quickly and positively when issues arise—is a critical component of our responsibilities. This is another factor used by regulators when evaluating our compliance programs, and you will note that recently, organizations have had heavy fines levied for not being responsive to patient or regulator inquiries within mandated deadlines.

Being responsive means acknowledging a request, question, or concern promptly; investigating impartially and with all due diligence the facts behind such requests or concerns; acknowledging issues if they are proven by facts; and moving swiftly to remediate verified problems. Do you get back to those who have raised an issue? Do you cooperate with audits and investigations? Do you close loops and document investigations? And, do you move quickly? Often, we cannot muster responsiveness on our own; others in the organization must assist. Is this in place for you? Do others understand that they must help when you ask? You have the right to demand that others support the mission to be responsive and give you timely, reliable information. With your governance structure and your partnerships in place, you should be getting what you need.

A force, not a function

Whether you work in a small office or have a compliance staff of 600,

your organization will take its ethical and compliance lead from you. Your personal opinions will be quoted, your judgment-calls scrutinized, your mistakes (yes, we make them) second-guessed. Clients, auditors, and regulators assess our performance too. Have all your functional components in place first, and once that's done, concentrate on being an open, energetic leader in your organization. Be a positive influential force, not a function or a title. People should know who you are. You must know their jobs, their challenges, and their concerns. It is essential they feel they can come to you, knowing you will listen intelligently and respectfully. They should see you preside over impartial, equitable, and thorough processes. They must see you champion improvements and take on big issues. Be discreet, reliable, and wise, as well as passionate about doing the right thing. Walk every piece of the talk.

This is the last, great personal challenge, which accepted and lived, takes your program to a higher level. Why? Action is compelling; leadership by example is the most powerful influence. Personally stimulating excellence throughout your organization can also be your most durable source of satisfaction, engagement, and creativity in your new role.

I hope you have an amazing and wonderful time. ■

Will the SEC's whistleblower bounty change employer/employee relationships?

By David Restaino, Esq.

Editor's note: David Restaino is a Partner in the Princeton, New Jersey office of Fox Rothschild LLP, where he provides compliance counsel in many subject matter areas, including regulatory aspects of health law. In addition, David's practice encompasses complex litigation in federal and state jurisdictions. As a former Deputy Attorney General, David also brings a working knowledge of government enforcement proceedings. He may be contacted by e-mail at drestaino@foxrothschild.com or by telephone at 609/895-6701.

Under regulations that took effect on August 12, 2011, the Securities and Exchange Commission (SEC) has given itself a new weapon to combat corporate fraud. In essence, whistleblowing employees in many different corporate environments have an incentive to notify the SEC of compliance issues—even if those employees have not utilized internal reporting systems—and earn themselves a huge reward.

The scope of the regulations is breathtaking. For example, if a publicly traded pharmaceutical company is illegally practicing off-label promotion of its products, a whistleblower who advises the SEC of this activity can receive up to 30% of a subsequent settlement of the allegations. Similarly, a private entity providing illegal kickbacks might, if it seeks to raise capital under certain Securities Act provisions, find itself subject to rules that protect a whistleblower from retaliation.

With settlements in many fields—be it pharmaceuticals, health care, or even violations of good manufacturing practices in the food and drug industry—exceeding hundreds of millions of dollars, and often billions, the impact of the new SEC rules will be immediate.

And that, apparently, is the whole point of Wall Street reform. While companies are already conversant in statutes like the False Claims Act and the Anti-kickback Statute, which use back-end penalties as a disincentive to fraud, the SEC can now attack the issue of corporate fraud from the other end, and use the people most likely to know about it (e.g., corporate employees) to root out the problem.

A summary of the Whistleblower Rewards Rule

Pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act (Wall Street Reform Act), adopted July 21, 2010, the SEC was empowered to adopt rules providing incentives for whistleblowers and also to provide them protection from retaliation.[1] The SEC rules were published on June 13, 2011, and became effective on August 12, 2011.[2]

Under the SEC rules, a whistleblower may be eligible to receive a bounty or reward, if he or she voluntarily provides original information that causes the SEC to commence an examination or open a successful investigation, or if the information significantly contributes to an ongoing investigation. The information cannot have been demanded by the SEC or known by the SEC from another source when reported. There are additional eligibility requirements. Among other things, the disclosures must lead to the recovery of more than $1 million (including "related actions" such as those brought by state attorneys general or by certain federal agencies).

The bounty is certain to raise a few eyebrows. For starters, eligible whistleblowers can get 10% to 30% of judgments that exceed $1 million, which should leave no doubt that the Wall Street Reform Act will encourage litigation against corporations. The actual value of a reward will depend on a variety of factors enumerated in the SEC rules (i.e., the reliability, completeness, and significance of the information provided, the degree to which it helped the enforcement action, and other assistance given by the whistleblower). Moreover, there is no requirement that a complaining employee first resort to available corporate compliance programs. Stated differently, internal reporting is not a pre-condition to award eligibility.

But, the SEC has provided some incentives for individuals to take advantage of internal corporate compliance programs: Voluntary participation in such programs increases the reward, and "full bounty credit" is given to persons whose internal efforts trigger a corporate disclosure to the SEC that results in a successful enforcement action.

The SEC rules are commonly viewed as applicable to public companies, but they go further. Also falling under the umbrella of the rules are broker-dealers and investment advisers as well as certain private companies seeking to raise capital under specified Securities Act provisions.

Fortunately, the SEC rules also contain some common sense exclusions, specifically that attorneys, directors, officers, compliance staff, and internal audit personnel are generally ineligible for rewards. There are, of course, exceptions to the exclusions, and those exceptions can reinvigorate what would otherwise be an ineligible event:

- 120 days have elapsed since the complaint was reported within the company, or
- the company is impeding an investigation, or
- action by the SEC is needed to prevent substantial injury to a company's or its investors' financial interest(s).

Finally, although not effective until August 12, 2011, the SEC rules are retroactive to tips received by the SEC after the July 21, 2010 adoption of the Wall Street Reform Act.

Are corporate compliance programs ready to be reformed?

Now that the dynamic has changed, it is time to refocus internal compliance programs, starting with those substantive areas where, statistically, fraud has been found more often:

- Financial statement manipulation;
- Practices made illegal by the Foreign Corrupt Practices Act, such as bribing another country's officials;
- Violations of the prohibition against illegal kickbacks, for example, payments by a hospital for illegal physician referrals; and
- Practices by a pharmaceutical manufacturer that influence decisions to prescribe a particular drug.

One study found that nearly one-quarter of fraud results in losses of more than a million dollars, that many instances of fraud are discovered by tips, and that anti-fraud controls do help reduce it.[3]

More important perhaps are the internal processes for rooting out fraud and other conduct likely to be the subject of a disclosure to the SEC. Internal compliance programs are not only designed to discover fraud, but they also *must* convince employees that any attempted fraud will be discovered, because the company is actually paying attention. Surprise audits and a program that encourages tips (e.g., a hotline that allows for anonymous disclosures) are important weapons in increasing vigilance and letting employees know that someone is always watching.

Equally important is a training program that teaches employees about common fraudulent activity and the ways to discover and report it. Such training should be frequently made a part of corporate newsletters or other employee

outreach so that its principles are fresh in the minds of those individuals considering illegal activity. In short, a company must make it clear that fraud will not be tolerated and its employees are empowered to detect it; anything less only invites trouble.

To ensure a top-down commitment, some companies have already established new regulatory Compliance Committees to "quarterback" their internal program. Those reviewing information generated by an enhanced compliance program should also have the expertise necessary to evaluate that information and the resources to seek outside expert assistance when appropriate.

Whatever the process, assigning compliance staff with a skill set adequate to assess technical information or, even more troublesome, vague disclosures, may be key to avoiding SEC involvement. Otherwise, the 120-day prohibition on certain staff members making disclosures to the SEC may be triggered.

Because those people contacted by internal investigators about known problems may still be considered an eligible whistleblower under the SEC rules, some thought should also be given to the practice of conducting internal investigations to minimize the potential for suggesting claims.

Additionally, counsel must also play a role in improving corporate compliance programs. Standard operating procedures and corporate manuals should be revisited to ensure they are consistent with the SEC rules and, just as importantly, to allow a corporation to discover illegal action and address it before the SEC gets involved. After all, preventing fraud was the point of the Wall Street Reform Act.

Similarly, company Marketing departments should continue to vigilantly ensure that publicly distributed marketing materials are accurate to avoid whistleblowing claims about "burying" negative information. Likewise, company policies regarding the use of social media should be adequately policed to avoid the distribution of inaccurate information. Companies can also compare their own performance to prior years or to their competitors, to the extent such information is available, as an indicator of compliance. Outliers in the data set can be targeted for additional auditing. Finally, fraud that is discovered internally must be met with immediate and intelligent punishment. The intelligence part is crucial, given the SEC rules' anti-retaliation scheme.

Anti-retaliation made paramount

Because the statute and the SEC rules include the concept of anti-retaliation, companies need to think twice about adverse employment decisions, even if justified, against complaining employees.

Retaliation includes the discharge, demotion, suspension, harassment, or discrimination against a whistleblower because of his/her lawful act in providing information to the SEC. Of course, that definition promises to cause no small level of consternation for Human Resources personnel faced with situations where, for example, a demotion is in order notwithstanding a whistleblower's revelations.

The eligibility for anti-retaliation is determined differently from whether an individual is eligible to receive a bounty. Whereas a reward is earned for disclosures leading to the recovery of more than $1 million, there is a lesser standard with respect to retaliation. Specifically, those employees with a "reasonable belief" in the truth of their allegations are under the umbrella of the anti-retaliation protections. Moreover, employees who have been retaliated against have the right to sue in US district court and can recover their counsel fees and litigation costs *and* be reinstated with double back pay.

Final thoughts … and a warning

Perhaps the biggest impact of the SEC rules will result from the misunderstanding of human behavior and litigation. Litigation

is about leverage and maximizing pressure and thus, a financial recovery. Couple that with the normal behavior of disgruntled employees who see a dim future with a company, and these forces will combine themselves into a whistleblower claim that by its very nature is designed for maximum adverse financial impact.

Fortunately, if the SEC operates in the manner suggested by the rules, it will ask questions first and shoot later, and only if necessary. Assuming as much, corporate compliance programs should improve and complaints will be made—and kept—internally. This can increase the number of internal investigations and decrease corporate liability. After passing through an initial period of doubts and hand–wringing, many corporations will reach the other side and find the Wall Street Reform Act had a positive impact on their organization and on the financial markets as a whole, much as Congress intended.

There is, however, a larger cost to the above-referenced benefits. Without question, the costs for implementing new compliance programs, including a method to handle whistleblower disclosures, will rise. Moreover, the incentives will be difficult for a disgruntled employee to pass up, a fact that is sure to increase complaints—and the costs of investigation.

Finally, the concept of anti-retaliation may be a factor in negotiating a resolution to enforcement actions. It may, at a minimum, require some adjustment of policies relating to the termination of disgruntled employees. ■

1. Public Law No. 111-203 § 922(a) (to be codified at 15 U.S.C. § 78u-6 et seq.) and § 924.
2. 76 Fed. Reg. 34,300 (June 13, 2011) (to be codified at 17 C.F.R. Part 240).
3. Association of Certified Fraud Examiners: "2010 Report to the Nations on Occupational Fraud and Abuse" at 4. Available at http://www.acfe.com/rttn/2010-rttn.asp.

Evolution of a compliance plan: Protecting revenue

By Susan Theuns, PA-C, CPC, CHC

Editor's note: Susan C. L. Theuns is the Administrative Director of a hospital-based multi-specialty group practice in Baltimore, Maryland. Susan may be contacted by e-mail at scltheuns@hotmail.com.

In an era of uncertainty and economic challenges, it may be time to revamp your compliance plan. Many may think that a robust Compliance department is just another business expense on the books, but it can actually give health care's bottom line a boost. Consider an effective overhaul of your compliance plan that includes a three-prong approach:

1. Getting back to basics
2. Preparing for the future
3. Protecting revenue

Getting back to basics

The Office of Inspector General (OIG) has detailed compliance plans for a variety of health care entities—hospitals, pharmaceutical manufacturers, ambulance suppliers, durable medical equipment (DME) suppliers, nursing facilities, Medicaid managed care organizations (MCOs), physician groups, hospices, clinical laboratories, home health agencies and so on. Interestingly, the OIG acknowledges that benefits of a compliance plan should include "enhancing health care providers' operations; improving the quality of health care services and reducing the overall cost of health care services."[1]

OIG set the basic guidelines of what needs to be included for each type of health care business and outline the minimal seven required elements. The elements differ by type of business but are mainly:

1. The development and distribution of written standards of conduct, as well as written policies and procedures to promote commitment to compliance.
2. The designation of a compliance officer and other bodies, such as a Compliance Committee.
3. The development of education and training programs for all affected employees.
4. The maintenance of a process to handle anonymous complaints, such as a hotline, and to protect whistleblowers from retaliation.
5. Development of a system to respond to allegations of illegal activities and enforcement of disciplinary actions against employees who have violated internal policies or federal or state law.
6. The use of audits and/or other techniques to monitor compliance and reduce risk.
7. The investigation and remediation of systemic problems and the development of policies addressing non-employment or retention of sanctioned individuals or companies/vendors.

As a basic pulse check, inspect how well all elements are being addressed in the current plan. Are they really being considered and applied on a regular basis? Can the efforts be supported with documentation?

In many cases, people are busy documenting generic or templated phrases into a compliance software program, but are not really accomplishing the element, goal, or purpose. Revisit the basics, do it with purpose, and make it useful. Set standards and have a way to make sure they are being met. These are minimum requirements, so meeting and exceeding them are a plus. Report formats with built-in queues will help ensure that all elements are addressed, whether manual or computer-generated.

A health care company should effectively monitor and audit weak or high risk areas. At a minimum,

these should be aligned and reviewed on an annual basis with the OIG Work Plan, plus any internal areas identified as risks, regardless of their inclusion in the current OIG Work Plan. Another question to ask is: Are there other OIG-identified businesses imbedded under the same tax ID number (TIN) that should be treated separately with their own compliance plan? For example, is there a physician group or pharmacy under a hospital that could benefit from its own focused plan? Is there a moderate- or high-complexity lab owned by the medical group? The standard compliance plan used may not cover vital areas of importance from the additional perspective(s).

Preparing for the future

Health care reform, payer policy changes, CMS regulations, conflict of interest, pharmaceutical manufacturers' changes, and other interdependent variable factors are in the process of morphing the industry. The Institute of Medicine (IOM) has identified six elements of 21st century healthcare[2] to be considered by all entities. As we look at the evolution of Pay for Performance (P4P) and other initiatives, it is already evident that these elements are being applied. The IOM tells us that health care should be (1) safe, (2) effective, (3) patient-centered, (4) timely, (5) efficient, and (6) equitable. These elements are an additional consideration in planning for the future of compliance as we all redirect and focus on where we need to be and what we need to do.

One of the unknowns is whether or not health care reform will follow through on federally mandating compliance plans and if or how their structure may change. Having a good solid plan in place now should make that transition easier when the time comes.

If your entity hasn't been through a Recovery Audit Contractor (RAC) audit, Medicare Administrative Contractor (MAC) audit, or the other alphabet audits like Zone Program Integrity Contractors (ZPICs) and Comprehensive Error Rate Test (CERT), it is most likely on your radar screen or sideview mirror. What can be done to protect and prepare for future audits? For the most part, what all of these are auditing are a "done deal." They are retrospective and the documentation has long been completed. You can use this information to identify areas that need to be improved or corrected through educational efforts for the next round of audits. If you haven't been through one yet, find out where they are focusing elsewhere around the country, and perform your own preliminary audits to develop corrective action plans. The sooner the better, and implementing corrective change to meet the documentation requirements will save you time and money. Procrastination in this area is costly in many ways.

We all know that ICD-10 coding is coming. ICD-10 preparation is a certainty and will impact everything from operations, work flows, billing systems, and forms. It will touch almost every aspect of health care, and that means compliance. Entities must have a game plan internally and not solely rely on consultants and vendors. Now is the time to pave the way and also help eliminate or reduce refunds resulting from future audits. ICD-10 is detail driven and so is the documentation for present-day RACs and other coding audits. This is the proverbial two-birds-with-one-stone scenario. Improved documentation to meet ICD-10 requirements today will also provide added protection for current audits. Health care entities should take advantage of the opportunity to prepare, train, and protect in one combined effort.

Keeping abreast of the trends and goals of adjunct services and businesses in the health care industry will help us all pace ourselves for where we will need to be as government deadlines approach. Examples are Medical Home, Accountable Care Organizations (ACO), demonstration projects,

Continued on page 50

 ...continued from page 49

Meaningful Use (e-prescribing and electronic records) and the dramatic shift from inpatient to outpatient care. Even if they have the best product to meet the current health care market today, tomorrow entities may find themselves scrambling to catch up and end up getting caught in the transition. Further, consider that the health care industry is one of the largest industries in the United States. In 2009, health care accounted for 17.6% of the US gross domestic product and is growing, according to CMS.[3]

Protecting revenue

Yes, compliance and revenue go hand-in-hand. In fact, the industry is pushing us all to become more efficient and save time and dollars wherever we can. Find out where compliance issues are costing your company money and close the gap. In a tandem effort, look for where compliance could make your health care entity money and go for it.

Revenue and reimbursement issues abound, even in the most successful companies. It is inevitable. We all deal with these issues to some degree, whether it is denials, write-offs, or an employee who isn't doing something quite right (or forgets to do something operationally). 2011 is time to look into the details and tighten up.

How often does someone look at denials and the real reasons for denials, not just for CMS, but for all payers? Look for trends and patterns in the denials and address them. It is amazing how the dollars can add up for forgetting a modifier, linking the wrong diagnosis, coding errors, lack of proper use of Advance Beneficiary Notices (ABNs), or failing to use the appropriate forms—even pre-authorization rules that vary from payer to payer within their

own product lines can impact the bottom line.

If billing is outsourced, find out the percentages and details for write-offs and denials by charges and by services; then track them and act where you can. Once an issue has been identified, it can be addressed and corrected—or avoided in many cases. Take it a step further and communicate your findings to those who are in the direct work flow from start to finish. Having additional eyes with checks and balances not only empowers people, but it makes them accountable. No one likes to work hard and then not get paid. Whether it's "never events" or just leaving a word off of a referral form, don't give anyone a reason not to pay.

Pay-for-Performance is another revenue area. Participation has been voluntary up to now, but the process will soon be mandatory by many payers. As traditional reimbursement decreases, this is one way to maintain past revenue levels from medical billing. Even on a voluntary basis, here is an opportunity to make money doing things that are probably already being done anyway. The key is to learn the process early so that the experience becomes a skill and process that is firmly in place when it becomes mandatory or critical. CMS is paying bonuses for participation in quality reporting and e-prescribing, but will begin withholding dollars in the very near future, if physicians are not onboard in the next year. Other payers are following suit, so current modes of reimbursement may soon be dependent on meeting performance standards. As with other areas of compliance, there must be documentation to support what is being reported, so this becomes a new area to monitor and audit by providers and payers alike.

Companies that pay doctors bonuses based on Relative Value Units (RVUs) should be aware of several scenarios that can cost big bucks to any health care organization. It can be a very flawed system. How RVUs are tracked and tallied and how the targets are set can be an unwelcomed expense that does not truly reflect reality. For example, the RVUs for a surgical assistant are the same as for the primary surgeon, but the reimbursement isn't.

Multiple procedure discounts will also impact reimbursement. If not scrutinized, reimbursement to providers for a procedure may end up exceeding the actual reimbursement from the payer. That's just not good business sense and such scenarios should prompt questions about fair market value or even Stark. RVUs tallied prior to Correct Coding Initiative (CCI) edits can be higher as well. Are physicians unbundling to game RVUs for bonuses? Until someone looks, no one knows for certain.

Summary

These are just a few examples of how getting back to the basics, preparing for the future, and protecting revenue can make a compliance plan more effective. In this environment, meeting the minimum isn't going to be enough. It's time to go beyond the requirements, expand the focus, and set higher expectations. There are a lot of good business opportunities under the compliance umbrella. Don't wait for the industry to direct your focus for you; keep your eyes open and look for innovative ways to make it work to your advantage. ■

1. Federal Register volume 70, No. 19, January 31, 2005
2. Institute of Medicine of the National Academies: Crossing the Quality Chasm: The IOM Health Care Quality Initiative. 1999. Available at http://www.iom.edu/Global/News%20Announcements/Crossing-the-Quality-Chasm-The-IOM-Health-Care-Quality-Initiative.aspx
3. CMS National Health Expenditure Data available at https://www.cms.gov/NationalHealthExpendData/25_NHE_Fact_Sheet.asp

In search of: The excluded

By Martha Ann Knutson, JD, CHC

Editor's note: Over the past fourteen years Martha Ann Knutson has served as the Compliance Officer for health systems in Maryland, Connecticut, and California. She can be reached at maknutson@gmail.com.

So far in 2011, the Department of Health and Human Services Office of the Inspector General (OIG) has announced settlements with five different health care organizations for employing individuals who have been excluded from participation in the federal health care programs. The continuing occurrence of such settlements, after more than a decade of experience with the related requirements, suggests either confusion in the provider community about responsibilities related to exclusion or that the processes related to identifying the excluded in a timely way are so challenging that occasional non-compliance is inevitable.

What's the duty?

In 1981, OIG took over administration of the process for excluding and reinstating individuals, entities, or companies from participation in the federal health care programs (e.g., Medicare, Medicaid, Tricare, veterans programs, etc.). The penalty of either time-limited or permanent exclusion may be levied in addition to civil monetary penalties or as a stand–alone administrative sanction for certain missteps. Exclusion is mandatory in certain cases, permissive in many others, but generally the conduct that triggers it contains an element of fraud or misconduct relating to a federal program, controlled substances, or patient neglect/abuse.

Exclusion is not limited to direct care providers. Currently there are lawyers, accountants, billing companies, and the comptroller of a tribal organization on the exclusion list. Additionally, excluded individuals may still be licensed as health care providers, because the actions leading to exclusion may or may not constitute a basis for revocation under the law of the state that licensed them. However those who have been excluded may not, during their exclusion, submit claims to the federal health care programs.

Since passage of the 1997 Balanced Budget Act (BBA), it has also become important for those not excluded to know if they employ, credential, or contract with the excluded, because no federal health care program payment can be made "for any item or service furnished…by an excluded individual or entity, or at the medical direction or on the prescription of a physician or other authorized individual who is excluded."[1]

Put simply, if a non-excluded health care provider bills the federal government for items and services that meet these definitions, it can find itself subject to all the various potential penalties for false claims—including exclusion—if it "knew or had reason to know of the exclusion."

Defining the boundaries

It's pretty clear when a billable service is delivered to a patient by or under the "medical direction" of an excluded provider. But in most settings, defining who, besides direct care providers, "furnished" a particular service can be more challenging, and the regulations do not include a definition.

In 1999, OIG issued a Special Advisory Bulletin to provide "guidance" to both the excluded and those who might employ or contract with an excluded individual or entity.[2] The BBA prohibited contracts or employment of excluded individuals or entities "for the provision of items or services for which payment may be made under" a federal health care program.[3] In the Special Advisory Bulletin, OIG made it clear that it would take a broad view of who "provides" items and services. According to OIG, those

billing the federal health care programs may not employ excluded individuals to provide "administrative and management services that are not directly related to patient care" but are a "necessary component" of providing such care. Trying to give guidelines for the many possible relationships between individuals and health care entities, OIG provided a series of examples of prohibited non-direct care services:

- Preparation of surgical trays
- Review of care plans
- Inputting prescription information for pharmacy billing
- Selling, delivering, or refilling orders for durable medical equipment
- Processing claims for payment
- Accounting
- Utilization review

The common denominator in the examples is that the wages, benefits, or contract price of the individual or entity providing the service was paid, at least in part, by revenues from a federal health care program. Thus, excluded individuals can be employed—but only if (1) they are exclusively paid by non-federal sources of funds and (2) the services they provide relate solely to non-federal program patients. The Special Advisory Bulletin also suggests the Advisory Opinion process as a route for testing if a particular relationship would run afoul of this prohibition—an offer that two organizations and one individual have accepted in the past twelve years.[4]

Finally, OIG stated that the "knows or should know" language in the BBA created an affirmative duty on the part of health care providers to check the program exclusion status of those they employ and contract with, before initiating the relationship, "or run the risk of civil monetary penalties (CMP) liability if they fail to do so." The agency urged program participants to check its online List of Excluded Individuals and Entities (LEIE) before hiring or contracting and "periodically" thereafter.

The LEIE is not the limit of the background checking duties of most providers. Exclusion lists are maintained by other federal and state agencies, which may impose duties to check them. For example, it is frequently suggested that a search of the federal Excluded Parties List System (maintained at www.epls.gov by the General Services Administration) should be part of a prudent background investigation. Additionally, many state Medicaid programs maintain their own exclusion lists in various formats.

Working this out in practice

Those who have been in the Compliance field for more than a day or two realize that the biggest challenge with requirements like this isn't understanding the expectations—it is making them part of day-to-day operational reality. In other words, who is going to check, how often, and how can the organization be sure this has been done?

Organizational challenges

At least three, and possibly many more, organizational "players" are involved in an effective exclusion-checking process. The Human Resource department (HR) traditionally oversees the background checks completed before employment. That same function may or may not be responsible for the engagement of contracted staff who work through an agency arrangement. And HR usually has little interest in being responsible for subsequent checking. The office responsible for credentialing medical staff, employed or voluntary, also has a role. Those involved in contracting and the department that has control over the vendor list of those to whom payments are made, have seats at the table.

One or more folks from the IT area will need to participate at least in the initial process design. The Compliance department, of course, has an interest in the overall process being workable and appropriately documented so that from time to time, it can be

Continued on page 54

 ...continued from page 53

tested. Legal resources may also be needed to draft contract expectations and remedies if the decision is made to rely, in whole or in part, on checks done by others.

Outsourcing the checking

Hiring someone else to check is one possible solution. Some vendors have packaged checking the OIG database with other pre-employment background checks of criminal and licensing records. That works for the initial check, but leaves the organization without expertise for the periodic follow-up checks. Outsourced checks are also often limited to those directly employed by the organization. What about the contractors and medical staff, volunteer board members, and agency staff? Someone (or maybe more than one individual) in the organization will still have to be responsible for periodically transferring the necessary data to the vendor and receiving the results of the check. It's very important to spell out responsibilities with the vendor in advance on what follow-up actions they—or you—will be responsible for taking when Dr. Smith or Nurse Jones looks like a "hit."

LEIE challenges

The database has more than 50,000 entries at present, with more than 1,700 of those added so far in 2011. The oldest entry dates back to 1978 (a physician from Lansdale, Pennsylvania—at least in 1978) and more than 2,700 of the entries relate solely to excluded businesses. Physicians are identified with the now defunct Unique Physician Identifier Number (UPIN) identifiers—and not the National Provider Identifier (NPI) numbers built into systems to be compliant with the electronic transactions standards over the past few years.

A backup verification system is on the website for double checking a possible name match with a Social Security number (SSN) or employer identification number (EIN), but first you have to find a "hit" based on the name.

So, say you want to enter into a contract with Metropolitan Ambulance and you search for that name on the list. You reassuringly won't find it—but, if previously the company was trading under Metro Ambulance, you might be contracting with an excluded provider. You cannot search the database by EIN or SSN, although doing so would greatly improve efficiency and the reliability of any match or pass finding. OIG can provide letters to non-excluded companies and individuals who have names similar to those appearing on the list. The non-excluded parties are happy to send you a copy of their OIG letter, but you have to first identify the issue and then find the person at the firm who knows about the letter.

Services provided on prescription
So, say a patient walks into your outpatient lab with a small white piece of paper torn from a physician prescription pad containing a handwritten (and signed) order for a complete blood count (CBC). The paper even contains a legible reason for the test. If you take the patient's blood, report the result to the physician, and bill the test to a federal health care program, did you violate your affirmative duty if it turns out that the ordering physician was excluded?

Reasonable compliance professionals can—and have—come to opposite conclusions on this one. Some argue that this is a service furnished "on the prescription" of an excluded provider and that, at a minimum, the program shouldn't pay. Others contend that unless the lab has either contracted with or employed the referring physician, there is no duty under the BBA to check for exclusion before submitting the claim. There is no written guidance at present from OIG on this point, although one presenter in the 2011 HEAT Provider Compliance Training sessions[5] suggested that such claims would not be reimbursable. (Another HEAT speaker confirmed that matters related to the exclusion responsibilities are the most frequent topic raised through the OIG self-disclosure process.)

At least one program safety contractor has taken the position that organizations do have a duty to screen for exclusion in such cases and not submit a claim for the service. (Following up to divert the next patient coming in with an order from the excluded doctor is yet another practical wrinkle.)

How often is "periodically"?
In the Supplemental Compliance Guidance for Hospitals,[6] OIG said that checking "routinely (e.g. at least annually)" was a mark of an effective compliance program. The same frequency has been used in more than one Corporate Integrity Agreement. Then in 2008, a letter issued to State Medicaid Directors set out an expectation that the Medicaid agencies would check the LEIE upon enrollment of providers and monthly thereafter. That monthly expectation is making its way outward in letters from those state agencies to providers as an expectation—greatly magnifying the "periodic" burden. More frequent checks, on the other hand, may mean less liability exposure for that person or contractor who somehow slips by in the initial check.

Stay tuned

In November 2010, OIG requested comments on the original Special Advisory Bulletin guidance, and received a few comments by January 2011.[7] For the most part, those comments focused on some of the practical issues discussed here. The comments also highlighted the need for a distinction in OIG's response to those providers who had a system to meet their affirmative duty and self-disclosed a failure of their system, and those who either didn't have an effective system or didn't self-disclose when they discovered an oversight. OIG is under no statutory obligation to issue additional guidance. So until it does, despite the ambiguities and challenges outlined here, the obligation still remains for each provider and supplier to have effective procedures to ensure that it doesn't and couldn't have known of an excluded provider in its midst. ■

1. 42 CFR § 1001.1901 (b)(1)
2. 64 FR § 52791ff (1999)
3. 42 USC § 1320a-7
4. See AO 07- 17, AO 03-01 and AO 01-06
5. HEAT Provider Compliance Training webcast, May 18, 2011, Washington DC. Available at http://oig.hhs.gov/newsroom/video.
6. OIG: Supplemental Compliance Guidance for Hospitals. January 2005. Available at http://oig.hhs.gov/fraud/docs/complianceguidance/012705HospSupplementalGuidance.pdf
7. All six are available at www.regulations.gov Docket ID HHSIG-2010-0003

Mentoring

By Marcella Henry

Editor's note: Marcella Henry is a Compliance Officer with Sunrise Community, Inc. located in Miami, Florida. Marcella may be contacted by e-mail at mhenry@sunrisegroup.org.

The Oxford Dictionary's definition of a mentor as a noun is "experienced and trusted adviser."

If you are charged with the responsibility of developing a compliance program for your organization, with very little guidance from your boss, what do you do? First you panic a little bit; but, you take a few deep breaths, and then focus on how to go about the development. That was me, six years ago.

The Internet is a wonderful source of information and leads you to many resources and opportunities. Two such sources are the Health Care & Compliance Association (HCCA) and the Society for Corporate Compliance and Ethics (SCCE). In these organizations, there are many experts who seem willing to assist. What I did immediately was join both organizations and start doing lots of research about developing a compliance program. An annual conference was approaching, and while looking through presenter names and bios, I tried to find someone whose background was compatible with that of my industry.

I then took a bold step and e-mailed this presenter, introducing myself and stating that I was "green" in the compliance industry and needed help. Within the hour, I received a very engaging and positive response from this person who offered to become my mentor. She extended herself to me while at the conference, and while attending the conference, we had a couple of meetings where she developed an outline for me on how to get started. She gave me assignments and time lines to get certain things accomplished that I was able to take back to my organization. These included development of the Compliance Charter, which she edited and then guided me for its approval by my board of directors.

As we continued to work together through phone conversations and e-mails, I felt very comfortable and knew that I could call on her for her support and encouragement on issues when I was stuck or just plain frustrated.

As time went on, I knew we needed her presence in our organization to continue the development of our compliance program for such things as the identification of our top risks and the development of a Compliance Work Plan, as well as in the development of the Code of Conduct. We were able to have her work with us in a consulting capacity to guide us. I shadowed her every move and saw how she went about getting the information from various department heads in our organization, and she worked with me in developing the Compliance Work Plan.

I learned from her the importance and necessity of the excluded persons review checks set forth in the Health and Human Services Office of Inspector General's website and the importance of making sure that the compliance program was designed to include the seven elements found in the Federal Sentencing Guidelines on how to have an effective compliance program.

An area of great emphasis for her was the development of employee training in knowledge and responsibilities for compliance. For an organization in multiple states, it is critical for the Compliance department to find creative ways to train all employees regularly, and also to have a presence in all organization locations. It is important to meet and educate staff about the compliance

program and to ensure their free access to all the necessary information.

I learned about the importance in having and chairing Compliance Committee meetings with an established purpose and frequency; to promote transparency and commitment from the executive management team in the organization, including the presence and participation of the President and CEO; and to have a prepared agenda, robust meeting minutes, and committee member assignments.

Throughout the years in which we have been working together, my mentor has evaluated various aspects of our program and given continued guidance.

The compliance program continues to evolve, because tweaking is needed when new laws and rules govern the program. My mentor is still very much available and willing to provide guidance with her knowledge and many years of experience. Today I introduce you to Cheryl Wagonhurst, Attorney at Law, and my mentor.

Thank You Cheryl! ■

People on the Move

Received a promotion? Have a new hire in your department?

If you have received a promotion, award, degree, accepted a new position, or added a new staff member to your Compliance department, please let us know. It's a great way to let the Compliance community know where you have moved on to, or who has joined the Compliance team. Send your job change information to: service@hcca-info.org

IG Levinson appointed to Government Accountability and Transparency Board

The White House has announced the launch of the Government Accountability and Transparency Board. As part of the Campaign to Cut Waste, the board will focus on rooting out misspent tax dollars and making government spending more accessible and transparent for the American people. Among those appointed to the board is Inspector General Daniel R. Levinson of the Department of Health & Human Services.

Former Compliance Officer appointed new Division Chief by Massachusetts Attorney General

Massachusetts Attorney General Martha Coakley has appointed a new Chief to lead her office's Non-Profit Organizations/Public Charities Division. Prior to this appointment, Mary Beckman served as the Compliance Officer and an attorney in the Office of General Counsel at Children's Hospital in Boston, where she specialized in conflict of interest issues, compliance with documentation and billing rules, and industry relations.

Frank Saputo joins PwC Health Industries

Frank Saputo, the former Chief Administrative Officer at US Oncology, has joined PwC US as a Managing Director in PwC's Health Industries Risk Assurance Group. Based in PwC's Houston office, Saputo brings more than 25 years of experience in the health care industry to the firm. In his new role, he will be working with health industries clients across the health continuum on risk and compliance programs.

WakeMed names Holloway Chief Compliance Officer

WakeMed Health & Hospitals is pleased to announce that Pandora Holloway has been named WakeMed's Chief Compliance Officer.

Maxim Healthcare Services, Inc., announces new appointments

Maxim Healthcare Services, Inc., an established provider of home health care, medical staffing, and wellness services, recently appointed Brett Barlag as Chief Financial Officer and Chief Strategy Officer and Timothy "Tim" Kuhn as Chief Culture Officer and Vice President.

START PLANNING NOW FOR

HCCA's 2012 Events

NATIONAL CONFERENCES

Managed Care Compliance Conference
February 12–14 | Scottsdale, AZ

Audit & Compliance Committee Conference
February 12–14 | Scottsdale, AZ

Compliance Institute
April 29–May 2 | Las Vegas, NV

Research Compliance Conference
June 3–6 | Austin, TX

Physician Practice/Clinic Compliance Conference
October 14–16 | Location TBA

Join us in Las Vegas

HCCA 2012 CAESARS PALACE Las Vegas, NV
COMPLIANCE INSTITUTE
April 29–May 2
www.compliance-institute.org
888-580-8373

To learn more about HCCA events, visit
www.hcca-info.org

Dates and locations are subject to change.

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

BASIC COMPLIANCE ACADEMIES

January 23–26
New York City, NY

February 13–16
San Francisco, CA

March 26–29
San Antonio, TX

June 4–7
Scottsdale, AZ

August 6–9
New York, NY

September 10–13
Location TBA

October 1–4
Boston, MA

November 5–8
Orlando, FL

December 10–13
San Diego, CA

RESEARCH BASIC COMPLIANCE ACADEMIES

January 30–February 2
San Francisco, CA

August 13–16
Boston, MA

PRIVACY BASIC COMPLIANCE ACADEMIES

March 12–15
San Antonio, TX

June 25–28
San Diego, CA

October 22–25
Orlando, FL

WEB CONFERENCES

Explore hot topics for compliance professionals with instant and up-to-date education from the convenience of your own office. HCCA announces new conferences regularly, and prior sessions are available for purchase on CD-ROM. Visit www.hcca-info.org for the latest updates.

REGIONAL CONFERENCES

Southeast
January 20 | Atlanta, GA

South Atlantic
January 27 | Orlando, FL

Southwest
February 17 | Dallas, TX

Alaska
March 1–2 | Anchorage, AK

Upper North Central
May 11 | Columbus, OH

Upper Northeast
May 18 | New York, NY

Gulf Coast
June 8 | Houston, TX

Pacific Northwest
June 15 | Seattle, WA

West Coast
June 22 | Newport Beach, CA

New England
September 7 | Boston, MA

Upper Midwest
September 14 | Minneapolis, MN

Midwest
September 21 | Overland Park, KS

North Central
October 5 | Indianapolis, IN

East Central
October 12 | Pittsburgh, PA

Hawaii
October 19 | Honolulu, HI

Mountain
October 26 | Denver, CO

Mid Central
November 9 | Louisville, KY

Desert Southwest
November 16 | Phoenix, AZ

South Central
November 30 | Nashville, TN

Upper West Coast
December 7 | Oakland, CA

Dodd-Frank: Much ado about nothing? A survey by HCCA and SCCE

By Adam Turteltaub, CCEP, CHC

In July 2010 the Dodd-Frank Act was passed, leading to a long and loud period of discussion about the Act's likely impact. Perhaps no area gained more headlines than the Act's requirement that whistleblowers receive between 10% and 30% of any potential fines over $1 million collected by the US government.

Some foresaw this provision triggering a firestorm of both legitimate and mal-intended claims. During the SEC's rule-making process, fears were also expressed that it would undermine existing compliance and ethics programs by encouraging employees to avoid internal mechanisms for reporting wrongdoing and take allegations straight to the SEC. A leading business group, in its comment letter to the SEC, wrote that the whistleblower provisions "...may undermine the functioning of effective corporate compliance programs by relegating them to the sidelines in the process of identifying and remedying violations of securities laws."[1]

To assess what has actually happened as a result of Dodd-Frank, the Health Care Compliance Association and the Society of Corporate Compliance and Ethics jointly fielded a survey to determine the impact, if any, the whistleblower provisions of Dodd-Frank have had on compliance and ethics programs. Our goal was to determine if the added incentives for employees to take their claims outside of the company were affecting the structure of compliance programs.

The survey revealed that relatively little has changed as a result of Dodd-Frank. Although companies are increasing communications to employees, the Act's whistleblower provisions have not led to wholesale changes to compliance programs. Instead they have primarily led to what most would likely welcome: increased communications to employees about what to do when encountering wrongdoing, and greater training of managers about how to handle reported wrongdoing.

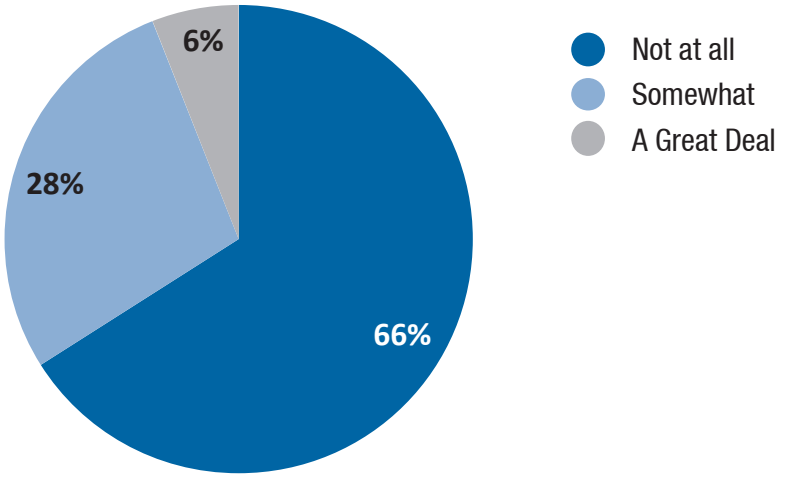
Survey results

Just 6% of respondents reported that Dodd-Frank had led to a "great deal" of change to their compliance program (see figure 1). To be sure, there were variations by industry type and company structure. For example, only 5% of healthcare companies reported their program had changed a great deal, but 11% of non-healthcare companies reported this level of change. But, on the whole, the Act does not seem to have led to wholesale transformations.

Continued on page 61

Figure 1

To what degree has your organization modified its compliance program as a result of Dodd-Frank?



REGIONAL CONFERENCES

HCCA'S REMAINING 2011

New England
September 9 | Boston, MA

Upper Midwest
September 16
Minneapolis, MN

Midwest
September 23
Overland Park, KS

North Central
October 3 | Indianapolis, IN

East Central
October 14 | Pittsburgh, PA

Hawaii
October 21 | Honolulu, HI

Mountain
October 28 | Denver, CO

Mid Central
November 4 | Louisville, KY

Desert Southwest
November 18
Scottsdale, AZ

South Central
December 2 | Nashville, TN

2012 REGIONAL CONFERENCES

Southeast
January 20 | Atlanta, GA

South Atlantic
January 27 | Orlando, FL

Southwest
February 17 | Dallas, TX

Alaska
March 1 - 2
Anchorage, AK

Upper North Central
May 11 | Columbus, OH

Upper North East
May 18 | New York, NY

Gulf Coast NEW!
June 8 | Houston, TX

Pacific Northwest
June 15
Seattle, WA

West Coast
June 22 | Newport Beach, CA

New England
September 7 | Boston, MA

Upper Midwest
September 14
Minneapolis, MN

Midwest
September 21
Overland Park, KS

North Central
October 5 | Indianapolis, IN

East Central
October 12 | Pittsburgh, PA

Hawaii
October 19 | Honolulu, HI

Mountain
October 26 | Denver, CO

Mid Central
November 9 | Louisville, KY

Desert Southwest
November 16 | Phoenix, AZ

South Central
November 30 | Nashville, TN

NEW!
Upper West Coast
December 7 | Oakland, CA

LEARN MORE AND REGISTER AT
WWW.HCCA-INFO.ORG

All 2011 Basic Compliance Academies sold out.

Register now for

2012 BASIC COMPLIANCE ACADEMIES

New York, NY
January 23–26, 2012

San Francisco, CA
Feb 13–16 , 2012

San Antonio, TX
March 26–29 , 2012

Scottsdale, AZ
June 4–7 , 2012

New York, NY
August 6–9 , 2012

Location TBD
Sept 10–13 , 2012

Boston, MA
Oct 1–4 , 2012

Orlando, FL
Nov 5–8 , 2012

San Diego, CA
Dec 10–13 , 2012

Learn more & register at
www.hcca-info.org

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

REGISTRATION FOR EACH ACADEMY LIMITED TO 75 ATTENDEES

HCCA's Compliance Academy is a four-day intensive program focusing on subject areas at the heart of health care compliance practice. Courses are designed for participants who have a basic knowledge of compliance concepts and some professional experience in a compliance function.

CHC® CERTIFICATION EXAM OFFERED FOLLOWING EACH ACADEMY

Be recognized for your experience and knowledge in health care compliance! Take advantage of the opportunity to sit for an optional CHC® exam on the last day of the Academy.

Even among publicly traded companies, which face the greatest risks from Dodd-Frank, only 8% reported that their compliance program had changed "a great deal," while 46% reported that their program had not changed at all.

One possible explanation for the relative lack of change was that anonymous helplines (hotlines) were already fairly ubiquitous. Overall, 90% of respondents reported that their employer already had an anonymous helpline in place. Among publicly-traded companies, 99% reported a helpline already present.

Some changes were made, though, as a result of Dodd-Frank. Anti-retaliation policies were reported changed by 13% of respondents. Increased communication to employees about opportunities to report wrongdoing were reported by 75%, and increased communications to managers about how to handle employee allegations of wrongdoing were reported by 46% (see figure 2). Looking to future changes, companies expect continued efforts in communication. Increased employee communication is expected by 74% of respondents and by 83% of those at publicly traded firms. Likewise, increased manager communication about handling allegations of wrongdoing is expected by 66% overall and 72% of respondents in publicly traded companies.

Conclusions

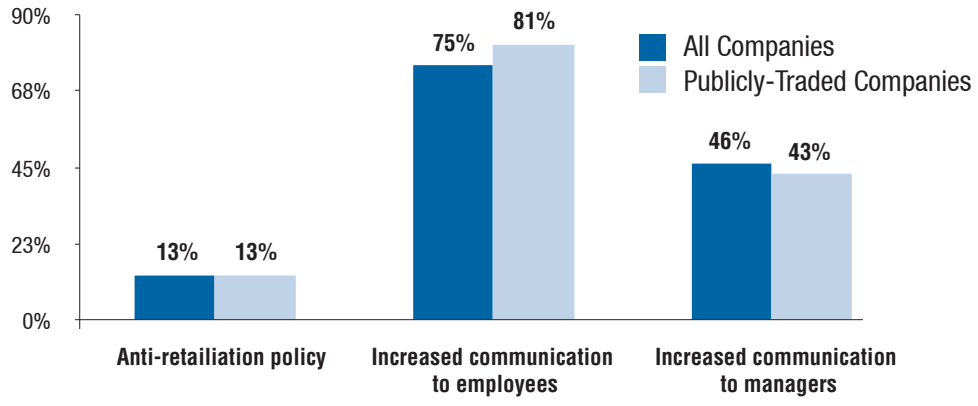
For most companies, the main impact of Dodd-Frank seems to be increased communications about internal opportunities to report wrongdoing. This is likely a positive development, regardless of the existence of Dodd-Frank. By making employees more aware of the opportunity to report wrongdoing internally, and the organization's eagerness for them to step forward, the business community will likely foster greater willingness of employees to raise their hands internally when they see malfeasance occur.

A second positive impact of Dodd-Frank appears to be increased training of managers. Research conducted in 2009 by the Ethics Resource Center, and co-sponsored by the SCCE, revealed that 46% of reports of perceived wrongdoing went to managers, compared to just 3% to anonymous helplines. With managers receiving such a large portion of allegations of improper behavior, it is critical that they understand how to handle those reports properly. Dodd-Frank appears to have accelerated the training process and may end up leading to faster, better handling of allegations.

In sum, Dodd-Frank does not appear, as of yet, to have made dramatic changes in the compliance landscape. To be sure, some of the provisions outside of the whistleblower arena will have an impact. Energy companies, for example, are affected by some of Dodd-Frank's requirements. But, on the whole, the Act does not appear to have been the watershed event for compliance and ethics programs that some predicted. ■

Figure 2

Percentage of respondents reporting company changes as a result of Dodd-Frank



1. Chamber of Commerce letter. Available on the SCCE website at http://www.sec.gov/comments/s7-33-10/s73310-189.pdf

HCCAnet

HCCAnet is the most comprehensive social network for health care compliance professionals. Subscribe to dozens of discussion groups and get your compliance questions answered. Offer your experience with your colleagues. Share your resources and policies in the libraries.

Resources

- HIPAA security assessment template can be found at www.hcca-info.org/Security Assesment

Mobile App

- Search for Mobile Membership Look for the logo
- Download app, then search for HCCAnet

Read some of the latest HCCAnet discussions:

HIPAA: Health Insurance Portability and Accountability Act Forum

❑ I've received mixed information and am wondering what your thoughts are on the topic. Is it a HIPAA violation to have a car magnet or sun visor in the window advertising your home health agency while visiting a patient in their home? www.hcca-info.org/9608

Critical Access Hospital CAH

❑ **Ethics Committees**

We are updating our Ethics Committee Policy and want to add statement that says something to the effect we retain the right to make final decision about whether we as an organization will comply with patient request or that just because the patient or family wants something does not mean the organization or physician must comply. Does anyone have policy they would be willing to share? Thanks. www.hcca-info.org/9626

Hospital Network

❑ **Two issues for which I would be very grateful for some guidance on...**

1. How do you handle the completion of medical record documentation and subsequent billing of claims when a practitioner must be terminated immediately? The ideal situation is that all documentation is completed by provders in a timely manner (like, immediately following the patient encounter), however that isn't always possible or followed. Provider is off for a few days, returns for duty, but has to be terminated and facility later discovers that the medical records of several recent patient encounters in the ED are incomplete - i.e. missing the terminated provider's signature on one or more pages, assessment half complete, etc.
2. Would anyone be willing to share their policy on the hospital's volunteer / Auxiliary program?

Many thanks to those who respond! www.hcca-info.org/9618

LinkedIn

❑ **Disposition of employee during investigation**

What do you do with an employee when your organization discovers what could be either a simple error or documentation falsification prior to the completion of an investigation? Does the employee get suspended, put on administrative leave, or continue to work until a determination is made? Thanks. http://lnkd.in/_-fG9t

2012 HCCA Compliance Institute Forum

Meet and Greet at 2012 Institute

I was reminded after seeing some general interest magazine covers already with hints of the upcoming holiday season that I guess you can't start too early in some respects. To that end...I am hoping to spark some dialogue with folks planning to attend the 2012 Institute in Las Vegas. I think this is a nice forum to share ideas and opinions on session offerings as well as even sharing feedback and thoughts on those sessions that folks attend at the Institute. So for folks looking to start getting connected, I hope folks find this particular thread within the eGroup interesting. **Onward!** www.hcca-info.org/9600

Documentation of HPI [Healthcare Performance Improvement]

Physician documentation

I am curious to get other opinions on the matter of documenting the HPI, especially in an EHR format. I have always been under the understanding that while the ROS and PFSH can be taken and documented by someone other than the physician, the HPI must be documented by the physician. Recently I have been getting some differing opinions and being that we are documenting in an EHR with a point-and-click method, my question is: Would it be appropriate for ancillary/clinical staff to document the HPI for the physician as long as the physician goes over the HPI with the patient and attests in some format that he/she was involved in the HPI process and asked the pertinent questions? www.hcca-info.org/9735

Contact Eric Newman at 952-405-7938, or e-mail Eric at eric.newman@hcca-info.org with any questions about HCCAnet. Also, ask Eric about the new HCCAnet mobile app for the iPhone, Blackberry, and Android devices.

HCCA Website News

Dodd-Frank Act survey

HCCA and SCCE conducted a survey that reveals that the Dodd-Frank Act had little impact, but instead is leading companies to communicate more to employees about reporting opportunities and to train managers on how to handle allegations. To see the results of this survey please check out www.hcca-info.org/surveys

A roadmap for new physicians

A booklet and PowerPoint are available for teaching physicians about the federal laws implemented to prevent fraud and abuse in the Medicare and Medicaid programs. This is available under the "Hot Links" on the HCCA homepage.

Potential interview questions for a compliance professional

Members can view a list of questions that may be asked at your next interview for a compliance position, online under the "Compliance Info" tab.

CHC practice quiz

Planning on taking one of the certification exams? There is 20 question quiz available online to help you get comfortable with the format of the questions. Practice exam available online under the Certification tab, click on "Practice Exam."

Compliance 101, Third Edition

Compliance 101 has been completely revised and updated. To order your copy online, please see the Books and Multimedia tab at www.hcca-info.org/compliance101.

Check out the dates for our 2012 Basic Academies

All of the 2011 Academies have sold out! If you want to become CHC certified in 2012, plan now to attend an HCCA Basic Compliance Academy and take the certification exam. Check our website and choose one of nine dates and locations for the 2012 Academies.

The Health Care Compliance Professional's Manual

SUBSCRIPTION SERVICE INCLUDED WITH PERIODIC UPDATES

- Hard-copy subscribers receive quarterly updates
- Internet subscribers receive updates as soon as they are issued

The Health Care Compliance Professional's Manual gives you all the tools you need to plan and execute a customized compliance program that meets federal standards. Available via print or the Internet, the Manual walks you through the entire process, start to finish, showing you how to draft compliance policies, build a strong compliance infrastructure in your organization, document your efforts, apply self-assessment techniques, create an effective education program, pinpoint areas of risk, conduct internal probes and much more.

The Health Care Compliance Professional's Manual shows you how to:

- Confidently use OIG publications and Federal Sentencing Guidelines to help you plan and execute a customized compliance strategy that meets strict federal standards
- Perform risk assessments within your program to help you uncover possible areas of risk
- Draft your own compliance policies that will form the basis for your organization's program
- Develop and reinforce a solid infrastructure, including guidelines for hiring the right personnel
- Design an effective education program that instills the importance of compliance
- Conduct your own internal probes to surface and cure questionable activities, thus mitigating possible penalties
- Keep continually up-to-date with the latest regulatory changes, including practical coverage of federal and state laws

MEMBER PRICE: $379
NON-MEMBER PRICE: $419

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Wolters Kluwer
CCH
Aspen Publishers

www.hcca-info.org | 888-580-8373

CT Advisory Board

Publisher: Health Care Compliance Association
888-580-8373

Executive Editor: Roy Snell, CEO, *roy.snell@hcca-info.org*

Contributing Editor: Gabriel Imperato, Esq., CHC

Editor: Margaret R. Dragon
781-593-4924, *margaret.dragon@hcca-info.org*

Copy Editor: Patricia Mees, CHC, CCEP
888-580-8373, *patricia.mees@hcca-info.org*

Layout and Production Manager: Gary DeVaan
888-580-8373, *gary.devaan@hcca-info.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.

New HCCA Members

Alabama
- TiJuana Halsey, Blue Cross and Blue Shield of Alabama
- Anita Helms, NHS Management

Arizona
- Fran Borg, Apogee Physicians

Arkansas
- Victor Sterling, Arkansas Dept Human Services

California
- Brent Baldwin, American Indian Health & Services
- Ofer Barlev, Palomar Pomerado Health
- Robert Bauchman, CareFusion
- Christy Bosse, Health Net, Inc.
- Laurie Cook, Inland Empire Health Plan
- Steve D. Fuss, Planned Parenthood of the Pacific SW
- Kevin R. Gillogly, WellPoint
- Laura Lane, Allergan, Inc.
- Jihane Marcos, Air Methods Corp
- Judith Marshall
- Sabrina R. Ruminer, Scripps Healthcare
- Alyssa M. Stillwell, Feather River Hospital

Colorado
- Tim Cashman, Valley View Hospital
- David Empey, Zynex Medical
- Mary Koretke, Pinon Management
- Alison Lakin, Univ of Colorado Denver

District of Columbia
- Caroline Conneely, FTI Consulting
- Randall Conrad, Veterans Affairs of Washington DC

Florida
- Rivki Beer, VITAS Healthcare
- Rhonda L. Bishop, Univ of Central Florida
- John Ford, MCS
- Felice Hersch, Martin Memorial Health Systems
- Robert Newell, Newell, Terry & Douglas, PA
- Heather Nydick
- Charlotte Parker, Gentiva Health Services
- Colleen Parkhurst, Mid-Florida Anesthesia Assoc
- Denise Perrone, Reliance Pathology Partners, LLC
- Peggy Pettit, VITAS Healthcare Corp
- Sandra Rodriguez
- Loretta Sayles, Reliance Pathology Partners, LLC
- Dee Sherwood, Raulerson & St Lucie Medical Center

Georgia
- Anita Culberson, Putnam General Hospital
- Barbara Lebow, Lebow Law Firm
- Marie Livingstone, Effingham Hospital
- Julie Rogers, Gentiva Health Services
- Joel A. Schuessler, DeKalb Medical
- Debbie Wolf, ProCare Rx

Hawaii
- Marilynn Hata, Marilynn Hata, LLC
- Leona Kiamahoe, Hawaii Pacific Health
- Lisa Tachibana, Hawaii Pacific Health

Indiana
- Angie M. Babb, St Vincent Health
- Melinda L. George, Deaconess Hospital
- Genevieve Koehler, Franciscan St. Anthony Health-Michigan City
- Gail Mahoney, Community Home Health Service
- Amie Martin, Proactive Medical Review & Consulting
- Marsha L. Shepherd, Memorial Hospital & Healthcare Center

Iowa
- Heidi N. Goodman, Iowa Medical Society
- Heather Rasmussen, Crawford County Memorial Hospital

Kentucky
- Marilyn L. Greenwell, Univ of Louisville
- Deborah Hile, Baptist Hospital East
- Bev Norton, Jewish Hospital St Mary's Healthcare
- Audrey Smith, Trilogy Health Services, LLC

Louisiana
- Jean Ann Hartzell Minzey, Healthcare Education Strategies

Maryland
- Claire Bowersox, Dynasplint Systems, Inc
- Pamela A. Daniels
- Melissa Erb, St Joseph Medical Center
- Janet McArthur, St Joseph Medical Center
- Jane McCaffrey, St Joseph Medical Center
- Natalie Stout
- Heather Woods, St Joseph Medical Center

Massachusetts
- Nancy L. Allen Scannell, MSPCC
- Meghan Colozzo, Tufts Medical Center
- Clifford Thomas D'Esmond,
- Loren Maloney, Fallon Clinic
- Stefanie N. Svoboda, DentaQuest LLC
- John J. Truitt, MDMED, Inc.
- Cindy Vredeveld, Massachusetts Eye and Ear Infirmary

- Michael J. Wagner, North Suffolk Mental Health Assoc

Michigan

- Becky J. Jacobson, U.P. Rehab Services
- Kimberly Segal, Karmanos Cancer Center
- Diane Wehby, Spectrum Health Continuing Care

Minnesota

- Dean Alexon, Allina Hospitals & Clinics
- Sally Amundson
- Jill L. Meemken-Pasch, BCBS of MN
- May Thao
- Cinda Velasco, MMIC Group

Mississippi

- Linda Robinson, Sonnenschein

Missouri

- Antionette Gillespie, BJC HealthCare
- William P. Hoffman, Greensfelder, Hemker & Gale
- Lisa M. Larson, BJC HealthCare
- Kyle Mead, Kansas City Community Center
- Sally E. Terrace, BJC HealthCare
- Amanda Wong

Nevada

- Dennis R. Dunn, Nevada Aids Project
- Mona Kaul

New Jersey

- Cathy L. Dennis, Kennedy Health System
- Joseph Kurland, Global Healthcare Services Group
- Vina Patel, UMDNJ-RWJMS
- Keith Roberts
- Carlotta Rodriguez, UMDNJ

New York

- David Anton, Access 7 Services
- Laura Eannace, Upstate Cerebral Palsy
- Edward Fried, The Institute for Family Health
- Sandra D. George, Regulatory Compliance Adjudication and Advocacy, Inc.
- Lisa Giglia, Catholic Health Services of Long Island
- Barrett Lorelei, The Saratoga Hospital
- Suzanne B. Pollard, Epilepsy Assoc of Greater Rochester
- Jessica Reed, Mount Sinai Medical Center
- Cayra M. Rosario, Montefiore Medical Center
- Yvonne Vazquez, Memorial Sloan Kettering Cancer Center

North Carolina

- Denice Anderson, Four Leaf Clover, Inc.
- Aubree Fisher, Novant Health
- Wendy J. Rogers, CaroMont Health
- Frank Watkins

Ohio

- Cynthia B. Blain, SS&G Healthcare Services
- Marjorie Flinn, Care Source
- Deborah Kocsis, Hospice of Central Ohio
- Julie Seitz, Julie L. Seitz, LLC
- Crystal Stevens, Nationwide Children's Hospital
- Tim Van Brandt, Mercy Health Partners

Oklahoma

- Angie Fodor, Dept of Veteran Affairs
- Paul S. King, Oklahoma State & Education Employees Group Insurance Board

Oregon

- Ellen Hampton, Salem Health
- Nicole R. Hough, St Charles Health System
- Kim F Nielsen

Pennsylvania

- Janice Aspey, Goodwill Industries of the Conemaugh Valley, Inc
- Tammy L. Banko, Magellan Behavioral Health of PA, Inc
- Helen Craigo, CL Cressler Inc
- Fotini A. Custer, Childrens Hospital of Philadelphia
- Deborah Datte, Abington Memorial Hospital
- Amy Derlink, Iod Inc
- Patrick Egan, Childrens Hospital of Philadelphia
- Leigh Ehrlich, PricewaterhouseCoopers
- Michael J. Fernan, Dickinson Center, Inc
- Thomas Genevro, Butler Health System
- Trina P. Grove, Lutheran Social Services of Southcentral PA
- Robert Haas, Eye Care Specialists
- Meg Lang, Executive Health Resources
- Bridget L. Morgan, Gateway Health Plan
- Rosemary Palusko, Goodwill Industries of Conemaugh Valley
- Robin M. Smith, Community Health and Dental Care, Inc

South Carolina

- Karen Sanford-Erikson, Columbia Gastroenterology Associates, PA

South Dakota

- Deana Fuller, Community HealthCare Association of the Dakotas

Tennessee

- Shea Bane, UnitedHealthcare Community & State Southeast HP
- Brett Burrell, Aegis Sciences Corp
- Waudea-Carene S. Farmer, HealthSpring

Continued on page 68

- Pam Frank, UnitedHealthcare Community & State Southeast HP
- Stephanie Gibbs, UnitedHealthcare Community & State Southeast HP
- Teresa Haddix, Parallon Business Solutions
- Jim Parks, Summit Medical Grp
- Alberto Pena, HealthSpring
- Christopher C. Puri, Bradley Arant Boult Cummings LLP
- Ashley Shields, Tennessee Medical Association

Texas

- Patsy Bachman, Wilbarger General Hospital
- Stephanie Butler, Cook Children's Health Care System
- David Chen, Texas Health Res
- Chad Copeland, Texas Tech Health Science Center
- Rudy Gomez, UTHSCSA-School of Nursing
- Mariko Hoffman, Universal American
- Julie Jolley
- Maria W. Kafatty, Medical Plaza Pharmacy
- Raj Kaushal, AccentCare
- Brian Kenny, Christus Health
- Adrian Larson, Val Verde Regional Medical Center
- Christy L. Naylor, Methodist Health System
- Allen Page, DLA Piper, LLP
- Parvinder S. Parmar, Baylor Health Care System
- Beth Taraban, TTUHSC
- Dudley T. Womble, Children's Medical Center Dallas
- Wanda Woody-Roberts, DePelchin Children's Center

Utah

- Jeff Clem, Health Care Insight/ Verisk Health
- Rustin Simons, Intermountain Sleep Disorders

Virginia

- Jacqueline Kniska, Virginia Commonwealth University
- Sarah Morabito
- Dorothea C. Scott
- Deborah Sikes, National Counseling Group, Inc
- Amy Walker, QSSI
- Nanette M. West, Kaiser Permanente

Washington

- Anthony Carter, Group Health Cooperative
- Michael Arnesen, Group Health
- Tracey Hugel, Family Care Network
- LaDon Linde, Sunnyside Community Hospital
- Lisa Savage, Yakima Valley FWC
- Sergio Vazquez, Yakima Valley Farm Workers Clinic

West Virginia

- Kimalisa K. Shamblin, South Charleston Cardiology

Wisconsin

- Colleen A. Chisnell, The Diagnostic & Treatment Center
- Laura Fairbanks, Spooner Health System
- Cheryl Knapp, Waukesha Memorial Hospital
- Rita Zehr, Advanced Pain Management
- David Zimmerman, Center for Health Systems Research & Analysis ■

Be Sure to Get Your CHC® CEUs

Articles related to the quiz in this issue of **Compliance Today**:

- **Pitfalls of and lessons learned: Provider documentation in the EMR**
  —By Ruth Krueger, page 12
- **They will never remember the vendor; you, however, are unforgettable...**
  —By Laurie Smaldon and Gretchen Hood, page 29
- **Will the SEC's whistleblower bounty change employer/ employee relationships?**
  —By David Restaino, page 44

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 CCB at 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. Only the first attempt to pass each quiz is accepted.

What could you do with The Power of Certainty?

Imagine being so consistent and accurate in outpatient charging, you'd always feel like you're on solid ground. Your CEO could launch cost-saving finance initiatives, without putting your hospital in the compliance hot seat. You could better preserve revenue, without compromising revenue integrity. And you could do it all, without unexpected trip-ups like takeback audit programs. This is the advantage of going with a proven revenue management solution. This is The Power of Certainty™.

Proven solutions for consistent, accurate outpatient charging.
www.lynxmed.com

LYNX medical systems™
now part of INGENIX.

HEALTH CARE COMPLIANCE ASSOCIATION'S 16th Annual

Compliance Institute

April 29–May 2, 2012 • Las Vegas, NV • Caesars Palace

EARLY BIRD REGISTRATION

Register by or on January 6, 2012, and save $575!

Join us in Las Vegas for the single most comprehensive compliance conference designed specifically to meet the needs of today's healthcare compliance professionals and their staff.

Preliminary Brochure now available online

Visit compliance-institute.org to download the brochure and register

HCCA
2012
CAESARS PALACE
Las Vegas, NV
COMPLIANCE INSTITUTE
April 29–May 2
www.compliance-institute.org
888-580-8373

Register now at
compliance-institute.org