HCCA HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

July 2015

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

Congratulations, Laura!

an interview with Laura Burke — our 15,000th member

See page 18

An intensive three-and-a-half-day program focusing on subject areas at the heart of healthcare compliance practice, designed for participants with a basic knowledge of compliance concepts and some professional experience in a compliance function.

Questions: jennifer.parrucci@corporatecompliance.org

Want to become Certified in Healthcare Compliance (CHC)®?

Take the optional CHC exam on the last day of the Academy.

CLE APPROVED

2015 Basic Compliance Academies

from the Health Care Compliance Association

REGISTER EARLY TO RESERVE YOUR PLACE
Limited to 75 for each Academy

SOLD OUT:
August 10–13 • New York, NY

LIMITED SEATS REMAIN:
September 14–17 • Chicago, IL

Sep 28–Oct 1 • Scottsdale, AZ

October 19–22 • Las Vegas, NV

October 26–29 • Nashville, TN

November 16–19 • Orlando, FL

Nov 30–Dec 3 • San Diego, CA

Learn more and register at
hcca-info.org/academies

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

by Roy Snell, CHC, CCEP-F

When is a compliance officer not a compliance officer?

Please don't hesitate to call me about anything any time.
612-709-6012 Cell • 952-933-8009 Direct
roy.snell@corporatecompliance.org
@RoySnellSCCE *in/roysnell*

A compliance officer checks the work of others for ethical and regulatory compliance. It is very similar to the role of an auditor. Auditors check the accuracy of financial statements. Auditors do not complete financial statements. If an auditor completed financial statements, the audit profession would say that person was not an auditor. Auditors are expected to be independent. You cannot be independent if you are checking the work you perform. An individual who performs work that must be occasionally checked for compliance with the rule of law cannot be called a compliance officer.


Snell

The whole purpose of creating the Compliance profession was to have an independent person check the work of others. There have been a few instances in which a compliance officer has been accused of wrongdoing by the enforcement community for submitting false or inaccurate documents to the government. Technically speaking, the individual submitting these documents to the government is not a compliance officer. The person completing the documents works in operations. They should have a different title and that person's work should occasionally be checked for compliance with the rule of law by a compliance officer.

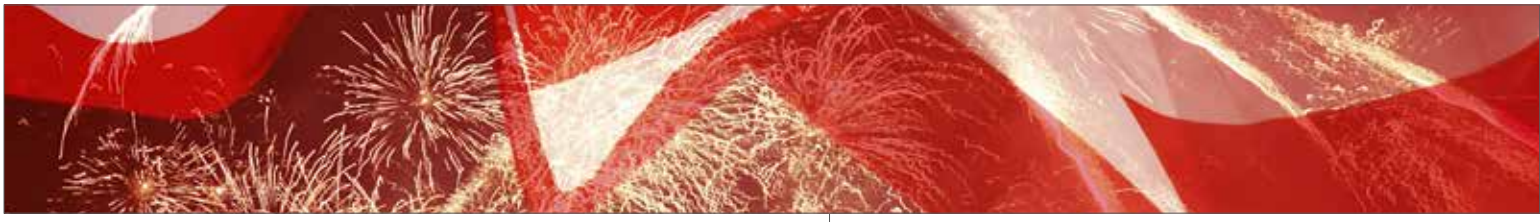
The Compliance profession is relatively new and not always well understood. Some companies are using the term "compliance officer" for jobs that do not fit the fundamental definition of a compliance officer. On occasion, a compliance officer is asked by their organization to manage some area of operations. Some compliance officers are asked to perform legal work. In these instances, the compliance officer should explain the need for independence to their organization and that taking over operations of any kind or performing legal work is not appropriate.

The Compliance profession is relatively new and not always well understood. Some companies are using the term "compliance officer" for jobs that do not fit the fundamental definition of a compliance officer.

This is also one of the many reasons why Compliance should be separate from Legal. You cannot perform legal work and then check the legal work you perform for compliance with the rule of law. There is no independence. Similarly the compliance officer should not have their annual review done by anyone whose work they must check. That would be as illogical as having the CFO audit their own work or perform the annual review of the people who audit them.

Contents

July 2015



FEATURES

COLUMNS

DEPARTMENTS

Compliance Today is printed with 100% soy-based, water-soluable inks on recycled paper, which includes 10% post-consumer waste. The remaining fiber comes from responsibly managed forests. The energy used to produce the paper is Green-e® certified renewable energy. Certifications for the paper include Forest Stewardship Council (FSC), Sustainable Forestry Initiative (SFI), and Programme for the Endorsement of Forest Certification (PEFC).

> You cannot manage COIs you are not aware of, so it is important to take steps that encourage employees to make these disclosures.

See page 20

ARTICLES

Compliance TODAY

Compliance Today (CT) (ISSN 1523-8466) is published by the Health Care Compliance Association (HCCA), 6500 Barrie Road, Suite 250, Minneapolis, MN 55435. Subscription rate is $295 a year for nonmembers. Periodicals postage-paid at Minneapolis, MN 55435. Postmaster: Send address changes to *Compliance Today*, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435.

VOLUME 17, ISSUE 7

Compliance & Ethics profession continues its dynamic expansion—SCCE and HCCA combined are 15,000 members strong

The Society of Corporate Compliance and Ethics (SCCE) and its sister organization, the Health Care Compliance Association, recently announced SCCE membership had grown to 5,000 members and HCCA membership had reached 10,000 members. It is apparent from this phenomenal growth that Compliance & Ethics is among the fastest growing professions both inside and outside the United States.

"When a small group of [healthcare] compliance officers sat down 19 years ago, we realized that there would be value in creating an organization that would help support our peers throughout healthcare. Back then having a thousand members seemed like an improbably large number. Now look at us with 10,000 members and part of one of the fastest growing professions in the world," said SCCE and HCCA Chief Executive Officer Roy Snell.

Upon SCCE achieving 5,000 members, Snell said, "This is a very significant milestone for Compliance & Ethics professionals. Many long doubted whether it was truly a profession of its own. It's now clear that it very much stands on its own."

The remarkable growth of the Compliance & Ethics profession in the U.S. and internationally speaks directly to the business community's recognition that compliance programs bring considerable value to their organizations.

"Compliance is integral to business now, no matter where an organization operates," said Snell.

Grant Thorton: Governance, Risk and Compliance Survey 2015

According to the report, "Grant Thornton LLP's 2015 Governance, Risk and Compliance Survey, which has previously only surveyed chief audit executives (CAEs), expanded this year to include responses from audit committee members. By casting a wider net for perspectives, the survey, now in its fifth year, pointed to subtle signs of a disconnection between these two groups of respondents. The responses suggest that CAEs and audit committee members see internal audit priorities differently.

"Asked to rank their focus on four types of risks, audit committee members cited their priorities as follows: financial, compliance, operational and strategic risks. It's not surprising that audit committees would be most concerned about risks related to financial controls, especially as it relates to the integrity of financial statements, considering that's where they have the most responsibility, accountability and exposure.

"On the other hand, CAEs ranked their risk focus as follows: compliance, operational, financial and strategic risks. The fact that audit committees viewed financial risks as the top risk, while CAEs ranked it third, hints at conflicting priorities."

For more: *http://gt-us.co/1G2Pr5t*

Read the latest news online ▶ www.hcca-info.org/news

Regulatory news

HHS OIG, HCCA, AHLA, and AHIA release joint guidance for healthcare boards

During his keynote address at the 2015 Compliance Institute, HHS Inspector General Daniel Levinson announced the release of "Practical Guidance for Health Care Governing Boards on Compliance Oversight," a joint collaboration between the Inspector General of the Department of Health and Human Services (HHS OIG), the American Health Lawyers Association (AHLA), the Association of Healthcare Internal Auditors (AHIA), and the Health Care Compliance Association (HCCA). This joint educational resource may assist governing boards of healthcare organizations to carry out their compliance plan oversight obligations.

On April 20, 2015, Modern Healthcare reported, "The guidelines state, 'OIG believes an organization's Compliance Officer should neither be counsel for the provider, nor be subordinate in function or position to counsel or the legal department, in any manner.'

"'Most healthcare organizations already have independent compliance officers, but there can be pressures to limit that independence,' Snell said.

"'We need the constant reminder that by definition a compliance officer isn't a compliance officer unless they're independent,' Snell said. 'We need to have it independent so leadership can get advice that comes from an unbiased perspective.'"

For more: http://bit.ly/1HeK2PF

To view "Practical Guidance for Health Care Governing Boards on Compliance Oversight" (PDF): http://bit.ly/1Pgku3K

To view Joint Press Release: http://bit.ly/1J9ys2k

CMS issues "Strategic Vision"

In an April blog post, the Centers for Medicare and Medicaid Principal Deputy Administrator and Chief Medical Officer Patrick Conway, MD, wrote about the Physician Quality Reporting Programs Strategic Vision. "This Strategic Vision, (http://bit.ly/1PgkzEe), describes a long-term vision for CMS quality measurement for physicians and professionals and public reporting programs, and how they can be optimized and aligned to support better decision-making from doctors, consumers, and every part of the health care system. The physician quality programs support our vision of a health system that achieves better care, smarter spending, and healthier people. These programs support incentives to providers, encourage improvements in care delivery, and deliver information to consumers.

"There are five principles we believe will ensure that quality measurement and public reporting play a critical role in improving the healthcare delivered to millions of Americans:

- Input from patients, caregivers, and healthcare professionals will guide the programs.
- Feedback and data drives rapid cycle quality improvement.
- Public reporting provides meaningful, transparent, and actionable information.
- Quality reporting programs rely on an aligned measure portfolio.
- Quality reporting and value-based purchasing program policies are aligned."

For more: http://bit.ly/1F4B2Av

Read the latest news online ▶ www.hcca-info.org/news

Online

Legal Education in Healthcare Compliance

with concentrations in:

- **Regulatory Analysis & Compliance**
- **Legal Nurse Consulting & Compliance**
- **Global Compliance & Ethics**

Master degree or graduate-level certificate available.
Accredited by the Compliance Certification Board.

Widener Law Delaware

302-477-2704 • delawarelaw.widener.edu

In Memoriam: Cleaster Ewing (September 29, 1959–March 14, 2015)

John Whittington *is Executive Vice President, General Counsel and Corporate Secretary for HealthSouth in Birmingham, AL.*

Our friend and colleague, Cleaster Ewing, known to her friends and family as Cle, passed away on March 14, 2015, following a brave and inspirational battle with cancer.

Cle was born and raised in El Dorado, Arkansas, where her parents still reside. She graduated from the University of Arkansas, Little Rock, and earned her master's degree in Public Administration from Florida Atlantic University. Most of you will remember Cle from the December 2012 issue of *Compliance Today*. The cover photograph captured Cle's beautiful smile and enthusiasm better than words could ever do. It is hard, if not impossible, to encapsulate the substance and the spirit of the person that I knew and worked with closely for almost five years. I recall that at our very first meeting in May 2010, I detected something about her that I could not identify, something that I recognized as good, interesting, and stimulating, but still something that I struggled to figure out. It took me years, but I finally concluded that Cle had this most incredible God-given gift—she commanded respect at all times. She didn't have to ask for respect. She didn't have to raise her voice or give you a threatening glare. She simply, by her actions, her words, her incredible beautiful smile, and that unforgettable infectious laugh, commanded respect. We always listened to her views and knew they were valuable and important, and we respected her for that. We knew she was unconditionally committed to making our compliance program the best it could possibly be. As Cle always said, "We're going to do this the HealthSouth way—which is—do the right thing, and do it the right way."

Yes, we learned a lot from Cle in the five short years we knew her. She always had our attention, and she definitely made our compliance program stronger than it was when she arrived. Most important is that we all at HealthSouth feel fortunate to have known her and to call her our friend.

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Research *Basic Compliance* Academies

Orlando, FL
November 2–5

With a wide range of research-related issues becoming hot topics with enforcement agencies, HCCA's Research Basic Compliance Academy® provides the opportunity to get information on many areas that affect research compliance officers and their staff on a day-to-day basis. A small audience encourages hands-on educational techniques, small group interaction, and networking.

questions:
jennie.nguyen@corporatecompliance.org

Learn more at
www.hcca-info.org/academies

Healthcare Privacy *Basic Compliance* Academies

Orlando, FL
November 2–5

HCCA's Healthcare Privacy Basic Compliance Academy® is comprehensive, covering a broad spectrum of laws and regulations that affect healthcare organizations: HIPAA privacy, general compliance, the Federal Privacy Act, and other privacy-related topics relative to healthcare. The faculty has many years of experience in healthcare compliance and is well-versed in healthcare privacy. The Academy is also helpful in preparing for healthcare privacy certification.

questions:
catherine.stollenwerk@corporatecompliance.org

Learn more at
www.hcca-info.org/academies

REGISTER EARLY
ACADEMIES FILL FAST

HCCA *conference news*

Healthcare Enforcement Compliance Institute

October 25–28, 2015 | Washington DC

www.hcca-info.org/HECI

HCCA is pleased to announce its first annual Healthcare Enforcement Compliance Institute coming to Washington DC, October 25–28, 2015.

Learn best and leading-edge practices for those involved in regulatory compliance at the Healthcare Enforcement Compliance Institute. The conference education will go beyond legal analysis to implementing systems that help ensure the law is followed. You will be provided practical advice from lawyers and compliance officers in an interactive forum that facilitates greater collaboration between the Legal and Compliance teams. Confirmed speakers include those from U.S. Depart of Justice, HHS-OIG, FDA's Center for Drug Evaluation and Research, U.S Depart of Health & Human Services, U.S. Attorney's Office, CMS, Office for Civil Rights, and the United States Sentencing Commission.

The conference features a full day of pre-conference workshops on Sunday and two days of the main conference on Monday and Tuesday. The Certified in Healthcare Compliance (CHC)® exam will be offered on Wednesday.

The agenda for the conference features three concurrent breakout sessions, covering a wide range of issues at the core of healthcare compliance. Compliance teams may want to send multiple members to make sure no essential topic is missed. Sessions will address issues such as: quality and healthcare fraud enforcement, FERA and the 60-day refund rule, whistleblowers, privilege in FCA litigation, self-disclosure, the board, and much, much more.

Be sure to make your plans early to take advantage of the early-bird discount rate. And don't forget to book your room at the Washington Hilton while space remains.

See full agenda and learn more at *www.hcca-info.org/HECI*.

Find the latest conference information online ▶ www.hcca-info.org/events

HCCA *website news*

Contact Tracey Page at 952-405-7936 or email her at tracey.page@corporatecompliance.org with any questions about HCCA's website.

Top pages last month

Home Page | Job Board | Events | My Account | About Membership

Number of website visits last month

58,154

Advertise

HCCA offers a variety of opportunities to market products and services to an audience of compliance professionals. This includes advertising in the magazine, the weekly newsletter, at our conferences, on our communities at HCCA*net*, or on our website. Each venue reaches thousands of people involved in compliance.

Visit *www.hcca-info.org/AdvertiseSponsor.aspx* to see all the opportunities and to choose the kind of advertising you're interested in. You'll then be taken to information covering that medium's reach, requirements, rates, samples, contact person, and submission forms.

Video of the month

What does a company need to do first to align its culture with its goals?

See this video and other videos on compliance culture at: *http://bit.ly/votm-ct-201507*

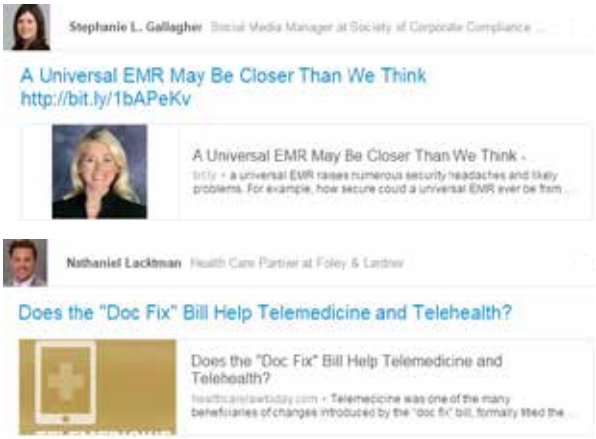
Find the latest HCCA website updates online ▶ www.hcca-info.org

HCCA *social media news*

Contact Stephanie Gallagher at 952-567-6212 or email her at stephanie.gallagher@corporatecompliance.org with any questions about HCCA social media.

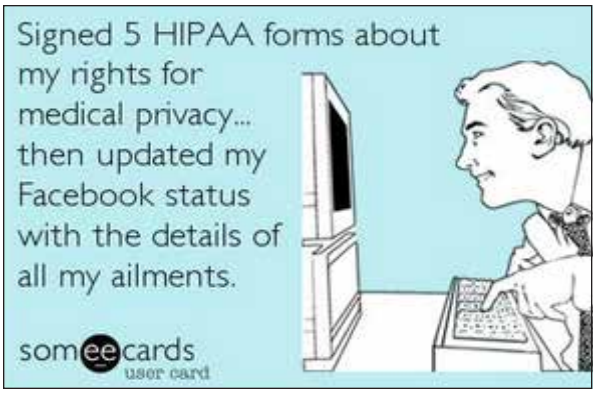
LinkedIn — *www.hcca-info.org/Linkedin*

Join us on LinkedIn—a business-oriented network with more than 240 million active users. With more than 20,000 members, our LinkedIn group fosters more than 75 new discussion posts every week. Some recent highlights:



Pinterest — *www.pinterest.com/theHCCA*

Check out our Pinterest boards for *HIPAA*, *ICD-10*, *ACA*, *Compliance Videos*, and using *Technology & Social Media* in healthcare, as well as map-boards for our major conferences (highlighting local restaurants, sights, and things to do in each of our conference cities). Our "infographics of the month" and much more can all be found on our Pinterest boards.



The C&E Blog — *www.complianceandethics.org*

Stop by our Compliance & Ethics Blog to check out discussions about hot topics and breaking news in compliance & ethics. Be sure to subscribe to have a daily digest emailed to your inbox. One recent post:

Twitter — *www.twitter.com/theHCCA*

Join 11,000+ others and follow HCCA for breaking news and insights. Some recent favorite tweets:

SlideShare — *www.slideshare.net/theHCCA*

We love sharing! Find informative and helpful presentations from every one of our conferences and presenters—free!

Find the latest HCCA*net*® updates online ▶ www.hcca-info.org/HCCAnet

PEOPLE *on the* MOVE

▶ **Donna Mackin** has been appointed Compliance Analyst for Mount Nittany Medical Center in State College, PA.

▶ The University of Texas MD Anderson Cancer Center (MD Anderson) in Houston, recently appointed **Allyson Kinzel**, JD, its Vice President and Chief Compliance and Ethics Officer; **Max C. Weber**, JD, MBA, its Associate Vice President and Deputy Chief Compliance Officer; and **Daniel E. Gospin**, JD, has joined The University of Texas MD Anderson Cancer Center (MD Anderson) as the Senior Legal Officer for Billing & Reimbursement Compliance.

▶ **Frances Hartman** has been named Compliance Officer at Wilbarger General Hospital in Vernon, TX.

▶ **Becky Lovelace**, CPA, CHFP, CHC, has been named Corporate Responsibility Officer for MissionPoint Health Partners in Nashville.

▶ Impax Laboratories, Inc., in Hayward, CA, announced the appointment of **Deborah M. Penza** as Senior Vice President, Chief Compliance Officer.

Received a promotion? New staff member in your department?

▶ If you've received a promotion or award, earned a degree or certification, accepted a new position, or added staff to your Compliance department, please let us know. It's a great way to keep the Compliance community up-to-date. Send your updates to: *margaret.dragon@corporatecompliance.org*

Help Keep Your Compliance Program Fully Staffed

List Your Job Openings Online with HCCA

It's hard to have an effective compliance program when you have openings on your team. Help fill those openings quickly—list your compliance job opportunities with the Health Care Compliance Association.

Benefits include:

- Listing is posted for 90 days to maximize exposure
- Targeted audience
- Your ad is also included in our biweekly HCCA Jobs Newsletter, which reaches more than 25,000 emails

Don't leave your compliance positions open any longer than necessary. Post your job listings with HCCA today.

Visit www.hcca-info.org/newjobs
Or call us at 888-580-8373

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

How do compliance officers of leading healthcare providers across America keep millions of employees compliant?

HCCS ONLINE COMPLIANCE COURSES

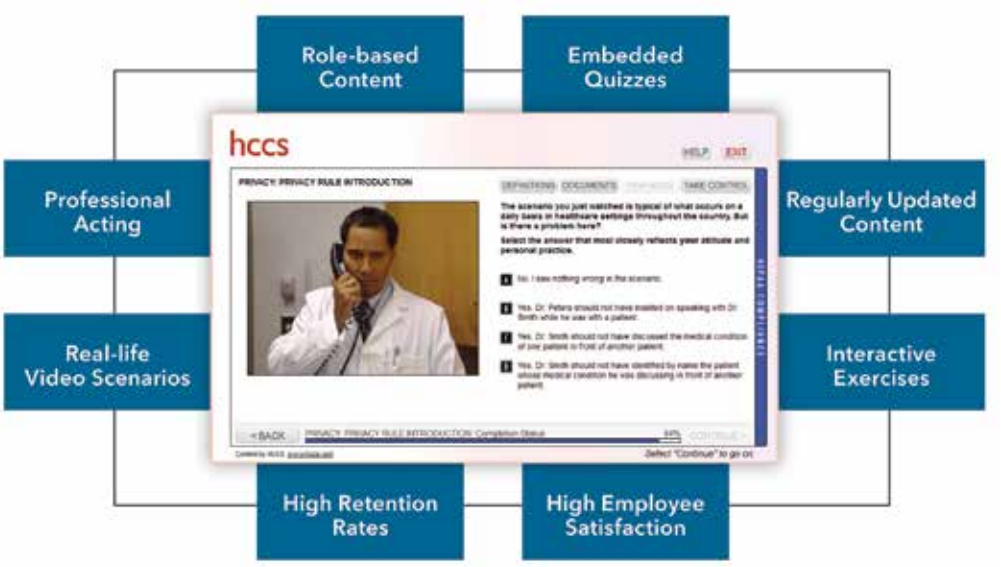
General Compliance Suite

Professional Compliance – Health System and Physician Office Versions
Corporate Compliance
HIPAA Compliance – Provider, Health Plan and Business Associate Versions
Deficit Reduction Act: False Claims and Employee Protections
Nursing Facility Compliance
Health Plan Compliance - ***New***
EMTALA - ***New***

Quality Improvement Suite

Patient Safety
Reducing Medication Errors
Documentation for Quality Care
Competency for Quality Care
Organizational Performance Improvement
Infection Control
Patient Rights
Patient Education
Bioterrorism and Disaster Preparation

The secret to success.



At HCCS we've always recognized the importance of people in the learning process. Computers may deliver the content, but real people administer and take the training.

Our online courses are designed to meet the needs of EVERYONE involved in the learning process. We rollout training quickly and efficiently. After the rollout, your staff won't complain of poor quality content or inattentive customer support.

> Role-based content ensures that learners receive information that's relevant to THEIR job function. **When employees pay attention, you reduce your risk.**
>
> Text-based courses with static, outdated information are boring! **Engaging, professionally designed multimedia content is more effective than page-turning text.**
>
> HCCS is the leading provider of online multimedia compliance and competency training courses with **over 2 million registered learners.**

All of this contributes to a better, more effective educational experience, greater compliance and reduced risk for your organization.

Research Compliance Suite

Grants and Contracts
Human Subjects Protection
Conflicts of Interest and Research Misconduct
Professional Relationships and Data Issues

Workplace Compliance Suite

Preventing Sexual Harassment for Healthcare Organizations
Identity Theft Prevention
Preventing Conflicts of Interest
Responsible Use of Social Media in Healthcare - ***New***

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

hccs
A *HealthStream*® Company

Laura Burke, CHC
Compliance Coordinator, Conflict of Interest
St. Jude Children's Research Hospital
Memphis, TN

an interview by Rory Jaffe

Meet our 15,000th member

Laura Burke *(laura.burke@stjude.org) was interviewed in April of 2015 by* ***Rory Jaffe*** *(rjaffe@chpso.org), Executive Director at CHPSO in Sacramento, CA.*

RJ: How did you first get involved in Compliance and Conflict of Interest (COI)?

LB: I became involved in Compliance and COI on a whim. The first job I held after graduating from law school primarily involved contract review and Human Resources. After a few years, I was considering potential career paths and learned about a newly created COI position at a large health system. I didn't have any experience with COI, but thought it sounded interesting, and I was excited to be the first person at that health system to hold that position. I thought it would be a fun challenge to start the COI program from scratch.

RJ: What has surprised you the most about working in Compliance?

LB: The pace at which the laws and regulations that affect compliance programs change has surprised me the most about working in Compliance. Successful compliance professionals must be flexible and willing to adapt, because the laws and regulations their programs are based on may change, and it may take significant effort to adjust the program to maintain compliance. In my position as a COI Coordinator, I regularly review COI literature and initiatives in addition to federal regulations and guidance to ensure the COI program at St. Jude is not only effective today, but down the road. In regards to COI, I have also been surprised at how willing COI professionals are to share information and materials and learn

from each other. I am fortunate to be able to participate in networking opportunities led by the Association of American Medical Colleges (AAMC). The AAMC hosts an annual meeting and provides a well-organized forum for COI professionals across the country to network and collaborate.

RJ: What attracted you to your current job?

LB: The opportunity to work at St. Jude attracted me to my job. It is an absolutely wonderful place to work. Although I do not work directly with our patients, I find it very rewarding to support the individuals who are at the forefront of advancing treatment for and eliminating pediatric catastrophic diseases.

RJ: How is the compliance reporting structure organized?

LB: The Compliance Office at St. Jude is led by our chief compliance officer, who reports directly to the hospital's president and chief executive officer, and also works with the board. A deputy compliance officer reports to the chief compliance officer. Several compliance coordinators report to the deputy compliance officer and have responsibilities related to education and training, auditing and monitoring, conflicts of interest, export controls, and research compliance.

RJ: How does COI compliance fit within the structure?

LB: I am the sole individual within the Compliance Office responsible for COI and I report to the deputy compliance officer, but I have the ability to review COI issues with the chief compliance officer. The COI Coordinator position at St. Jude is housed in the Compliance Office, rather than a department with more research oversight, because all St. Jude employees are subject to the COI policy and associated procedures. I also coordinate and prepare materials for a COI Committee at St. Jude, which reviews individual and institutional COI issues.

> Successful compliance professionals must be flexible and willing to adapt, because the laws and regulations their programs are based on may change, and it may take significant effort to adjust the program to maintain compliance.

RJ: What is the organizational thinking behind having a dedicated person addressing COI?

LB: The COI program at St. Jude is based heavily on the revised Public Health Service (PHS) COI regulations, which are designed to promote objectivity and avoid bias in PHS-funded research. The National Institutes of Health, Food and Drug Administration, and Centers for Disease Control and Prevention fall under the umbrella of PHS-funded research. The institutional COI program also relies on standards set forth by the Association for the Accreditation of Human Research Protection Programs. These regulations require institutions receiving funds from PHS to collect specific information from all individuals participating in the design, conduct, and/or reporting of PHS-funded research to ensure they do not have financial interests and/or relationships that could negatively impact, or bias, that research. This information must be reviewed at certain times during the research

process. The COI policy at St. Jude also extends the disclosure thresholds set forth in these regulations to employees not conducting research.

RJ: What are the largest risk areas from a COI perspective?

LB: One of the largest risk areas of COI is individuals not disclosing interests and relationships they are required to disclose per federal and/or state law and regulation as well as institutional policy. For a COI program to be effective, individuals must be willing to disclose the interests and relationships they are required to disclose. If an individual does not disclose such an interest or relationship and it is discovered after required COI reviews were conducted, it could cause issues for an institution regarding the PHS research funding it receives.

The Physician Payments Sunshine Act, also known as Open Payments, adds another wrinkle to this risk. Now that financial relationships between physicians and industry are being listed on the Centers for Medicare & Medicaid Services (CMS) public Open Payments website, it's possible an institution could discover a significant financial relationship between a physician and industry that should have been disclosed, but was not. Institutions must encourage their physicians to make accurate and complete disclosures to avoid such a situation.

To encourage employees to make accurate and complete disclosures, institutions should display their commitment to keeping COI disclosures confidential and protected, and have a secure means for employees to make their disclosures.

RJ: Can you give an overview of how you manage COI risks?

LB: Management plans are used to manage identified COIs. Management plans are intended to serve as guides for employees and outline appropriate ways for employees to complete employment responsibilities related to their COI and interact with the organization employees COI is associated with, including listing activities to avoid. For example, it is standard language in St. Jude management plans to require an employee to not disclose confidential St. Jude information to the organization the employee's COI relates to.

> One of the largest risk areas of COI is individuals not disclosing interests and relationships they are required to disclose per federal and/or state law and regulation as well as institutional policy.

Certain COI issues may be reviewed by the COI Committee prior to a management plan being implemented. The COI Committee at St. Jude has members with a variety of expertise: Research, patient care, legal, compliance, and technology transfer. An employee subject to a management plan may be more willing to work with you when the COI Committee supports the management plan.

RJ: What advice would you give other compliance professionals about controlling COI risks?

LB: Encourage employees to disclose interests and relationships they are required to disclose. You cannot manage COIs you are not aware of, so it is important to take steps

that encourage employees to make these disclosures. At St. Jude, we share with employees when it is time for them to complete their annual COI disclosure using postcards, posters, and email announcements. You must also be willing to assist employees who have questions about what to disclose or how to do it, or you may discourage them from making disclosures. Be prepared to discuss why these disclosures are important. Some employees do not want to share personal financial information or feel the disclosure process is cumbersome, but if you help them understand why they need to make these disclosures, they may be more willing to disclose.

Most individuals do not think a financial interest or relationship will impact how they complete their employment responsibilities, but research shows it might.

RJ: What is the greatest challenge to having a successful COI compliance program?

LB: Helping employees understand why COI is important can be a challenge. Most individuals do not think a financial interest or relationship will impact how they complete their employment responsibilities, but research shows it might. Helping employees understand COI disclosure and management plans are intended to help them avoid situations where their judgment appears to be impacted or biased helps employees believe in the COI program.

You also need to be willing to do what it takes to educate your workforce on COI. I have conducted several COI education and training sessions at St. Jude, and it is important to tailor these sessions to the audience. For example, employees working in food service will have a different perspective on how COI applies to them than employees conducting research.

RJ: What is your most significant accomplishment so far?

LB: Employees see me as a resource for COI questions and concerns. I constantly receive emails and phone calls from employees who want to make sure they are completing their COI requirements correctly, or have questions about a relationship they are considering entering into with industry. To be a successful compliance professional, I think it is crucial for employees to see you as approachable and capable of assisting them. This is an image the St. Jude Compliance Office strives to project.

RJ: What is most rewarding about your job?

LB: The COI program at St. Jude applies to all employees, so I've had the opportunity to meet and work with individuals at all levels within the organization. I find it very fulfilling to help employees meet their COI requirements and build strong relationships outside the Compliance Office.

RJ: What relationships do you think are critical for the ethics and compliance program to be effective?

LB: For a Compliance Office to be effective, not only does it need to have strong working relationships with departments it collaborates with, but, possibly most important, it needs to have strong ties to an institution's workforce as a whole. When I facilitate the compliance presentation at the hospital's new employee orientation, I always mention the Compliance Office wants employees to feel they can approach all members of the Compliance Office with questions and concerns, that we are a

resource for all employees. I want employees to feel comfortable approaching me with questions or asking for assistance. If employees don't feel comfortable with compliance staff, they may not be willing to share potential compliance issues.

RJ: What do you wish your colleagues outside of the Compliance department better understood about compliance?

LB: The intent behind a compliance program is not to pull employees away from their work. Regarding COI, researchers may have to complete several disclosures, depending on the type of research funding they receive, and it can begin to feel burdensome.

RJ: What might someone be surprised to know about you?

LB: I majored in Anthropology in college and received my Tribal Law Certificate in law school. My original career goal was to work for the Bureau of Indian Affairs within the Department of the Interior.

RJ: What would you tell someone who is thinking about working in this field?

LB: There may be more than one way to appropriately address a compliance issue. And don't be afraid to network! Bouncing ideas off other compliance professionals may lead to some of your best ideas.

RJ: What do you like to do when you aren't working?

LB: I recently became engaged, so I need to start planning my wedding!

Know what's right, right now with

ComplyTrack®

Confidently manage risk and drive compliance across your enterprise in the face of constant regulatory change with the visibility, controls and workflows **ComplyTrack** provides. Our up-to-date regulatory content and unparalleled expertise are woven into the **ComplyTrack** question sets and controls for complete decision support. Created and supported by experts in healthcare risk, audit, and compliance, your tailorable **ComplyTrack** SaaS solution is scalable and quick to deploy.

complytrack.com

Wolters Kluwer
Law & Business

by Catherine Boerner

Does the compliance officer need to be on the executive leadership team?

Catherine Boerner *(cboerner@boernerconsultingllc.com) is President at Boerner Consulting, LLC located in New Berlin, WI.* *in/catherineboerner*

Many compliance officers feel frustrated because they are not considered members of the executive team and are not invited to weekly executive team meetings. Sometimes compliance officers even find out about purchases of new clinics, or even hospitals, long after the decisions have been made. By not being at the executive table, you miss out on strategic planning decisions and are not offered the opportunity to identify and raise potential compliance concerns or risks. If you were at the table earlier in the process, you might have been able to suggest that leadership consider the compliance risks and establish some controls at the outset to mitigate these risks. It is so nice to be proactive once in a while, isn't it? We all seem to be in a reactive mode for much of our job.

Boerner

I argued and fought for most of the last 17 years for compliance officers to be on the executive leadership team and at the table. I even once had a CEO tell me that if their current compliance officer had to be at the executive leadership weekly meetings, then they were going to have to find a different compliance officer. In the end, we were able to compromise and provide the compliance officer with agendas to the meetings and, if he felt the need to attend, he could. So, why should we "exhale" and accept our fate, in some organizations, as not regularly being at the executive leadership meetings? I had a seriously compelling argument from a CEO last year on this very point. The CEO explained to me that she needed her compliance officer to be independent and not afraid to ruffle feathers with her senior vice presidents when needed. She valued the compliance officer's ability to say it like it is and not back down when she felt challenged about why she needed more information or assurance that controls were, in fact, in place to mitigate compliance risks. This CEO did not want the compliance officer to get "too close" to the executive team individuals, and perhaps, the politics, where she could be influenced to back down, due to building those relationships. I have to admit it was the first good argument on this topic I had heard. Whether you agree or not, it is an interesting perspective to consider.

If you were at the table earlier in the process, you might have been able to suggest that leadership consider the compliance risks and establish some controls at the outset to mitigate these risks.

MANAGE YOUR COMPLIANCE PROGRAM WITH COMPLIANCE 360:

Claims audits and denials by payers, new policies and procedures to reflect ever-changing laws and regulations, scrutiny of physician relationships, Medicare compliance audits, and managing HIPAA privacy rules are just a few of the issues creating unprecedented compliance and financial risks that healthcare organizations must manage effectively. With so much complexity – and so much at stake - you need a comprehensive, unified solution that helps you identify and fix the gaps… before something falls through them.

To learn more about Compliance 360 for Healthcare: please visit www.compliance360.com/healthcare

GET THE 360° VIEW.

www.compliance360.com

SAI GLOBAL
COMPLIANCE 360® GRC SOLUTIONS

by Michael J. McCarthy and Andrew W. Mahler

When risk assessments become exhibits: Are you prepared?

» Patients whose protected health information (PHI) has been breached are successfully suing providers in state courts.

» These lawsuits are usually based on claims that the provider negligently handled PHI, using HIPAA as the standard of care providers owe their patients.

» Schedule meetings with the appropriate people in your organization to discuss new legal trends.

» Change your perspective when writing risk assessments or incident reports—they could become exhibits in a lawsuit.

» Get input and counsel from others in your organization, such as the Office of General Counsel, when you have to make a tough call.

Michael J. McCarthy *(mccarthy-michael@cooperhealth.edu) is the Director of Integrity and Compliance at Cooper University Health Care in Camden, NJ.*
Andrew W. Mahler *(amahler@email.arizona.edu) is the HIPAA Privacy Officer for the University of Arizona in Tucson, AZ.*

Before you sign-off on a medical device audit or a privacy or security risk assessment after an incident, consider this sequence of events: The next time you see this document could be with outside counsel as you both prepare for a deposition. In this scenario, opposing counsel is a veteran class-action attorney. Even worse, you realize there is a mistake you overlooked in prior reviews. As compliance professionals, we cannot afford to put our organizations in this position.

Several years ago, the scenario above was highly unlikely. Plaintiffs suing healthcare providers after a breach routinely failed, because the Health Insurance Portability and Accountability Act of 1996 (HIPAA) does not provide a private cause of action. In other words, a hospital could not be sued after an information security breach, for example, if the only allegation was a HIPAA violation. Although HIPAA's prohibition of private lawsuits has not changed, plaintiffs in a few states have found success, arguing HIPAA as a standard of care, in lawsuits against healthcare providers. This trend has placed privacy and security officers, compliance professionals, and in-house counsel in the hot seat. Now, it is perhaps more important than ever that your organization develop clear and organized strategies to protect itself when conducting risk assessments. (Please note that we use "risk assessment(s)" to mean an organization's process of assessing an impermissible use or disclosure of PHI.)


McCarthy


Mahler

Strategies will vary between organizations but such strategies should always be developed in close consultation with general counsel and key stakeholders.

There is still no private right of action

Generally, HIPAA does not provide a clear cause of action for a plaintiff(s) to file a lawsuit based solely on the Privacy, Security or Breach Notification Rules.[1] Furthermore, HIPAA, as a federal law, preempts any contrary, less restrictive provision of a state's privacy or security laws. These hurdles raise a key issue for covered entities, their business associates, and plaintiffs: Even if a plaintiff were to successfully argue that a claim, based solely on

a violation of HIPAA could succeed, he/she would then have to prove that the violation caused harm.

Indeed, this is one question that has not been fully answered by courts: Even if a court were to determine that a covered entity or business associate owed the plaintiff a specific duty, how would one appropriately measure damages resulting from a breach of PHI? Although it might be apparent (depending on the facts and circumstances of a particular case) that information privacy or security has been breached, it will be very challenging for a court to calculate damages because of the inherent difficulty of linking a particular information breach to identity theft or other harm.

Consider the following example: You have lunch at a chain restaurant and then purchase a new microwave at a big box store. Later that afternoon, you go to your doctor for a routine visit, which was billed to your insurance provider. Of course, you used your credit card for all of the purchases and services. Several weeks later, you are notified that several of these organizations were victims of a breach and that your information might be compromised. How would you or even an expert definitively determine the exact source or organization responsible for keeping your information secure?

To make things more difficult for plaintiffs, many victims of identity theft might not know that they are victims for months, or even years. This timeframe makes it even more difficult for a plaintiff to demonstrate that the identity theft can be directly linked to a particular system or organization. Despite recent courtroom victories for the plaintiffs discussed below, these issues and questions have yet to be fully resolved.

So, what has changed?

Within the past year, the media has published reports of breaches from a variety of sources and concerning a variety of types of personal information. Several notable breaches involved Target (2014), Home Depot (2014), and Anthem and Premera (2015). Although the general public may not be aware of the unique differences in regulations and oversight pertaining to information used, disclosed, or maintained by different types of organizations, the public perception is that breaches are inevitable and they are largely helpless when their information is accessed or stolen. It is clear, however, that several state courts are starting to notice. Plaintiffs and their lawyers, arguing in several state courts, have reaped benefits from cases involving data breaches of personal information.

> …public perception is that breaches are inevitable and they are largely helpless when their information is accessed or stolen.

This is not a legal article; however, it is vital for privacy and compliance professionals to be aware of the arguments driving these new cases. Broadly speaking, the theories that were argued in these cases share the claim that HIPAA should be used as a guide to what patients might expect from their healthcare providers and that significant deviations from these practices could constitute negligence on the part of the providers. Two recent cases, decided in 2014, demonstrate new strategies and developments surrounding the use of HIPAA in the courtroom. Such strategies should be closely examined in order to understand how to protect your organization and implement new practices.

Byrne v. Avery

In *Byrne v. Avery Center for Obstetrics and Gynecology, P.C.*,[2] the Connecticut Supreme Court held that the plaintiff could proceed with a state claim that a HIPAA covered entity breached a duty of confidentiality. In this case, the covered entity, Avery, received a subpoena from Byrne's ex-boyfriend's lawyer requesting Byrne's medical records, which were at-issue in a paternity suit. Avery did not obtain a valid HIPAA authorization from Byrne nor allowed her an opportunity to quash the subpoena before disclosing Byrne's PHI.

The Connecticut Supreme Court, in the opinion issued on November 11, 2014, found that Avery not only acted negligently when its employee disclosed PHI, but was also liable to Byrne for intentional infliction of emotional distress. Perhaps most importantly for compliance professionals, the Court also held that HIPAA does not preempt similar claims related to a breach of patient privacy. In other words, HIPAA may inform the applicable standard of care in certain circumstances. In at least ten states, courts have shown a willingness to use HIPAA as a standard of care: Delaware, Indiana, Kentucky, Maine, Minnesota, Montana, North Carolina, Tennessee, Utah, and West Virginia.

Walgreen Co. v. Hinchy

On November 14, 2014, the Indiana Court of Appeals upheld a $1.44 million jury trial verdict against Walgreens Co., when a pharmacist impermissibly disclosed information about a customer, Hinchy, who is the ex-girlfriend of a Walgreens pharmacist's husband and a Walgreens customer.[3] The allegations at issue were that Hinchy's pharmacist viewed her prescription history and shared that information with her husband, who then shared that information with others. Hinchy sued the pharmacist and the pharmacist's employer, Walgreens, alleging that Walgreens was responsible for improper actions of its employee.

Specifically, Hinchy argued that Walgreens breached Indiana's common law duties of confidentiality and privacy. (Hinchy also alleged that Walgreens was negligent in not properly training the pharmacist, but the Court threw out that allegation before trial.)

The Indiana Court of Appeals upheld Hinchy's claim that HIPAA should be used as the standard of care for those state common law duties. Additionally, the Court held that Walgreens was responsible for the improper actions of its pharmacist. Although Walgreens could further appeal this case, an appellate court ruling creates binding legal precedent in Indiana state district courts. Undoubtedly, lawyers representing victims of breaches of PHI in other states will urge their states to follow Indiana's lead.

In addition to these two cases, there are several ongoing, class-action lawsuits that have yet to be resolved. One notable case to watch is the current lawsuit involving Community Health Systems, following their large PHI breach. Another incident to follow closely is the circumstances surrounding the breach affecting customers of Anthem, Inc. Each of these recent breaches has triggered lawsuits; now judges across the country will be asked to resolve these issues

What can you do?

Collaborate

If you have not yet talked to your general counsel about the risks posed by these new cases, this should be your first step. No one in your organization understands how to better prepare for these risks than your general counsel, but keep in mind that protecting the organization should always be a shared goal. Neither compliance professionals nor general counsel want their organization surprised by a controversial risk assessment or audit result. Moreover, documents relating to—or created in preparation for—these events may present

a litigation risk. These documents should be reviewed by those who will handle potential litigation or other possible negative consequences. In the past, discussions surrounding risk assessments and accompanying documentation mainly surrounded managing the breach, purchasing new software, or hiring staff; now, there is the very real threat of a class-action lawsuit. If that happens to your organization, all hands will be on deck.

Learn to write for a new audience

There is a big difference (even though there shouldn't be!) between documenting a breach assessment for an internal report and writing one with the knowledge that it could be an exhibit in a future lawsuit. It is important that compliance professionals "think like a lawyer" when conducting assessments and writing reports, knowing that these documents may be seen by a larger audience.

There are at least two possible methodologies for handling this risk.

One type of methodology that many organizations adopt is based in the idea that compliance professionals should always "show their work." In other words, organizations ask that incidents, findings, and conclusions are carefully and completely documented, usually in the form of a memo. The compliance professional will, wherever possible, cite to internal policies, regulations, Office for Civil Rights (OCR) settlement agreements, or guidance in the documentation. However, while this approach will surely demonstrate the office's effectiveness to internal stakeholders, it is important to note that the work could also be shown to outside audiences. The compliance professional may be asked to prove that he/she has meaningfully considered all possibilities and, for valid reasons, did not believe that a breach or other violation was reportable. In this methodology, the goal is to be able to clearly articulate that, although others may disagree with the conclusions; the final determination was made diligently, in good faith, and based on relevant regulations and guidance.

Another type of methodology is for organizations to adhere to the maxim of "less is more," by simply answering "yes" or "no" to questions on a form. If the organization utilizes this method, the same form should be used consistently in every incident and breach assessment. In addition, compliance professionals must be confident that such forms include all relevant assessment metrics. This type of document could be preferable for litigation purposes, because it does not expose the compliance professional's thought process (i.e. "showing the work"), which could be viewed by a general counsel as providing unnecessary or potentially harmful information. In this case, the organization may decide that it is preferable to use simple forms and not provide opposing counsel fodder for cross-examination. However, an inherent risk with this model is that it may be difficult to remember many of the more complex details of the assessment. Some organizations using this approach argue that the thought process can be saved for later time; that is, if or when the assessment is called into question.

> It is important that compliance professionals "think like a lawyer" when conducting assessments and writing reports…

Remember: Regardless of the model your organization chooses, use forms and documents consistently.

Tips to protect your organization

- Do not assume your general counsel is updated about these cases and new legal trends. Schedule a meeting and craft an action plan to deal with privacy and security issues that might present a litigation risk.
- When you sit down to write risk assessments or incident reports, change your perspective. Be prepared for a larger audience to review your work.
- Is there a reason you write risk assessments, risk analyses, etc. a certain way? Have a good answer to this question.
- If you have to make a tough call, you must get input from others in your organization. Reach out to departments such as the Office of General Counsel or Information Security.
- You do not need a JD, just common sense. You know that OCR can potentially review your work as part of an audit or investigation and, hopefully, you have prepared accordingly. There may be new threats, but you have the tools to succeed.

1. Department of Health and Human Services, Office of the Secretary: Standards for Privacy of Individually Identifiable Health Information. 45 CFR Parts 160 and 164. December 28, 2000. 65 Fed. Reg. 82601. Available at: http://bit.ly/1cY1989
2. *Emily Byrne v. Avery Center for Obstetrics and Gynecology, P.C.* Supreme Court of South Carolina, SC 18904, 2014 WL 5507439. Nov. 11, 2014. Available at: http://bit.ly/1cY1ach
3. *Walgreen Co. v. Abigail E. Hinchy*, Indiana Court of Appeals No. 49A02-1311-CT-950, Nov.14, 2014. Available at: http://bit.ly/1LEj1fR

Get high-quality, convenient, inexpensive education and networking opportunities. Don't miss the chance to attend an HCCA Regional Conference in your area!

2015 Regional Compliance Conferences

Don't miss your chance to attend one of HCCA's remaining 2015 Regional Compliance Conferences

September 11 • Boston, MA

September 18 • Minneapolis, MN

September 25 • Overland Park, KS

October 2 • Indianapolis, IN

October 9 • Pittsburgh, PA

October 15–16 • Honolulu, HI

October 23 • Denver, CO

November 6 • Louisville, KY

November 13 • Scottsdale, AZ

November 20 • Nashville, TN

December 4 • San Francisco, CA

December 11 • Houston, TX

hcca-info.org/regionals

questions: beckie.smith@hcca-info.org

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

by Isabella R. Edmundson, JD, CHC, and Lauren S. Gennett, JD, CHC

RAC forecast: Are we in the eye of the storm or are sunny skies ahead?

» The RAC program has been in a lull since June 2014, and the award of the new Medicare Part A/B RACs has been delayed due to a pre-award protest.

» On December 30, 2014, CMS announced several program changes aimed at reducing provider burden and increasing transparency in the RAC program.

» Some of these program changes may be beneficial, but much depends on how CMS will implement and enforce the changes.

» The changes will not be implemented until the new RAC contracts are awarded, which for certain contracts may not be until at least 2016.

» Providers should prepare for RAC reviews to begin again in full force once RACs are able to resume regular reviews, including patient status reviews.

Isabella R. Edmundson *(iedmundson@kslaw.com) and* ***Lauren S. Gennett*** *(lgennett@kslaw.com) are Associates at the law firm of King & Spalding in Atlanta.*

In today's complex healthcare environment, providers are facing increasing scrutiny of federal healthcare payments by various Medicare and Medicaid contractors. Perhaps the most significant of these contractors is the Medicare Recovery Audit Contractor (RAC). The national Part A/B RAC program began in 2010 with the goals of ensuring accurate payment to Medicare providers and offering education to providers to prevent future overpayments. Although these are certainly admirable goals, in practice, the RAC program has demonstrated several fundamental flaws and, according to some, done far more harm than good.

One of the most influential features of the RAC program is its compensation structure. Importantly, the Centers for Medicare & Medicaid Services (CMS) pays RACs a contingency fee based on a percentage of the improper payments corrected by the RACs. This has shaped RAC behavior by incentivizing RACs to deny claims and to target high-dollar claims. The resulting RAC "feeding frenzy" contributed to a large number of appeals, which in turn has caused a well-publicized backlog in the Office of Medicare Hearing and Appeals (OMHA).[1]

Edmundson

Gennett

The RAC program is now at an important juncture. The first national Medicare Part A/B RAC contracts lapsed in June of 2014, and the RAC program has since been in a lull, pending the award of the next round of RAC contracts. Protests from incumbent RACs have led to significant delays in awarding the next round of RAC contracts. Additionally, CMS has announced several program changes aimed at addressing certain concerns raised by providers. At this point, it is unclear how these developments will shape the future of

the RAC program. Is the current lull just the eye of the storm? Will the RACs be back in full force? Or will the changes announced by CMS mean sunnier skies ahead for providers? This article aims to provide some practical insight on what is next in the contractor forecast.

Contract delays and extensions

For the review of Medicare Part A and B claims, the United States is divided into four RAC jurisdictions, Regions 1 through 4. There is also a Region 5 RAC, which was created for the second round of RAC contracts and operates nationally to review durable medical equipment, prosthetics, orthotics and supplies (DMEPOS), and home health/hospice (HH/H) claims.

As noted, the first round of Part A/B RAC contracts lapsed in June 2014. Originally, CMS intended to award the new Part A/B RAC contracts in February 2014. However, during the rebidding process, CMS encountered delays as a result of a pre-award bid protest filed by an incumbent RAC, CGI Federal Inc. (CGI). CGI filed a lawsuit contending, among other things, that the new RAC contract terms contained in CMS's Request for Quotes (RFQ) were inconsistent with customary commercial practices and unfairly restricted competition. Specifically, CGI challenged a provision of the new contracts that would delay the time at which RACs would receive contingency payments on a claim until after the claim is upheld on the second level of review—a program change that many providers believe is a step in the right direction, in light of the concerns surrounding the RAC incentive structure.

In August 2014, the Court of Federal Claims denied CGI's challenge. CGI immediately appealed and, in an unexpected turn of events, on September 2, 2014, the Court of Federal Claims granted CGI's request to prevent CMS from awarding the new RAC contracts for Regions 1, 2, and 4 until after CGI's appeal has been resolved.[2] On March 10, 2015, the Court of Appeals for the Federal Circuit reversed the Court of Federal Claims and found in favor of CGI. The case was remanded back to the Court of Federal Claims for additional proceedings.

This legal challenge is not expected to end soon; CMS has indicated that it expects the CGI litigation to continue well into late summer of 2015.[3] Accordingly, in August 2014, CMS announced modifications of the contracts with the prior RACs to allow them to restart certain reviews. The reviews authorized by this "limited restart" of the RAC program were mainly automated reviews with a limited number of complex review topics selected by CMS.

This legal challenge is not expected to end soon; CMS has indicated that it expects the CGI litigation to continue well into late summer of 2015.

By November 2014, CMS remained optimistic that the new RAC contracts for the jurisdictions unaffected by the CGI protest (i.e., Region 3, the one Part A/B contract not impacted by the CGI challenge, and Region 5, the new national DMEPOS HH/H RAC) would be awarded by the end of 2014. CMS was able to partially adhere to this timetable. On December 30, 2014, CMS announced that it had awarded the Region 5 DMEPOS HH/H RAC contract to Connolly, LLC (Connolly). However, due to a bid protest filed by Performant Recovery, Inc. (an incumbent RAC), it is not clear when reviews will commence.[4]

The status of the Region 3 contract remains uncertain, although CMS has stated that it hopes to award the Region 3 contract shortly. In addition, in light of the continued delays

with the remaining Part A/B RAC contracts, on December 24, 2014, CMS announced another extension of the Part A/B RAC contracts until December 31, 2015.[5] On December 30, 2014, CMS also announced various program improvements, detailed below, that would become effective for the new RAC contract awards.

Patient status reviews

Further complicating this landscape is the Two-Midnight Rule Probe & Educate period, which prohibits RACs from conducting patient status reviews of claims with dates of admission between October 1, 2013, and September 30, 2015. Like the RAC contract awards, the Probe & Educate period has its own muddied history of extensions. However, absent any additional extensions, the Probe & Educate period will expire on September 30, 2015.

At this point, it is not clear how these developments (the RAC contract extensions, the RAC program changes, and the expiration of the Probe & Educate period) all intersect. CMS has not yet publicly clarified whether the prior RACs operating under the contract extensions announced in December 2014 will be permitted to audit patient status claims once the Probe & Educate period expires. Although CMS has not confirmed details of the new RAC contracts, it is likely that once the new contracts are awarded, the new RACs will be able to look back and review inpatient status determinations with dates of service from September 30, 2015 to December 31, 2015.

Nevertheless, providers can expect that RACs will pursue inpatient status reviews aggressively as soon as they are permitted to resume such reviews. According to CMS, 94% of the dollars recovered by RACs involve inpatient hospital claims.[6] Because the RACs have been prohibited from reviewing patient status claims (the bread and butter of reviews for many RACs) for dates of service after October 1, 2013, there is little doubt that when the gates open and RACs are able to review patient status claims again, the RACs will pursue such audits with renewed vigor. Accordingly, providers would be well advised to conduct proactive internal reviews, particularly with respect to compliance with the Two-Midnight Rule for patient status determinations, so that they are prepared for what may be another RAC feeding frenzy.

RAC program improvements effective with new contracts

As mentioned above, on December 30, 2014, CMS published an updated list of RAC program improvements that are designed to enhance oversight, reduce provider burden, and increase program transparency.[7] The improvements will be effective with each new RAC contract awarded after December 30, 2014, including the recently-awarded DMEPOS HH/H RAC contract. In light of the delays in the new Part A/B RAC contract awards, some providers may not experience the implementation of these changes for months, or even until 2016.

According to CMS, the announcement of the program changes "marks the beginning of the new Recovery Audit contracts and is the start date of the implementation of many improvements to reduce provider burden and increase transparency in the program."[8] Although CMS's efforts to respond to provider concern and refine the RAC program are laudable, unfortunately, many of the program improvements may not result in substantial changes for providers.

To organize our discussion of the program changes, we have summarized a selection of significant improvements below, and divided our analysis into two categories: (1) changes aimed at limiting the scope and reducing the burden of RAC reviews; and (2) changes aimed at adjusting the RAC incentive structure to enhance the quality and accuracy of RAC decisions.

Reducing the scope and burden of RAC reviews

Additional Documentation Request limits based on a provider's compliance

Based on this enhancement, providers that have better compliance rates with Medicare rules should experience fewer RAC reviews, instead of the one-size-fits-all Additional Documentation Request (ADR) limits for providers of similar size that have historically been in place. However, CMS has not clarified exactly how this compliance rate will be determined.

Diversifying established ADR limits across all claim types of a facility

This development attempts to ensure that a provider with multiple claim types (e.g., inpatient, outpatient) is not disproportionately impacted by RAC review of one claim type (e.g., all of a provider's inpatient rehabilitation claims reviewed or all inpatient claims reviewed). The practical significance of this development will be shaped by how CMS establishes and enforces such ADR limits.

Incremental application of ADR limits to new providers

This enhancement instructs RACs to incrementally apply ADR limits to new providers under review to ensure that such providers currently have staffing levels sufficient to timely respond to RAC requests for documentation. This stands to be a significant improvement for certain providers, because one of the unfortunate consequences of the RAC program has been the disproportionate impact on providers without RAC experience, and providers with fewer resources to address RAC reviews. Historically, when certain RACs identified providers with repeated technical or documentation errors, RACs would quickly launch a full-scale review, sensing fertile ground for claim denials. This sort of overwhelming situation could distract the provider from remedying the compliance issue identified, while the provider was required to quickly respond to repeated, voluminous RAC reviews. Again, the practical significance of this development will turn on CMS's standards and enforcement.

Broader review topics and reviews of certain topics based on referrals

This change requires RACs to broaden review topics to include all claim and provider types and to review certain topics based on referrals, such as an OIG report. CMS enacted this change in response to concerns that RACs focus their resources on inpatient hospital claims. Until CMS provides more details regarding this improvement, it remains unclear what the requirements will entail and how CMS will enforce varied reviews.

Limiting the RAC look-back period

This change limits the RAC look-back period to 6 months from the date of service for patient status reviews if the hospital submits the claim within 3 months of the date of service. This has the potential to have great impact and to remedy a serious flaw in the RAC program. To comply with timely filing rules, hospitals are required to submit claims within one year from the date of service. RACs, on the other hand, have historically had a 3-year look-back period. As a result of these varying timeframes, when a RAC determined that a certain claim should have been billed as an outpatient claim, the hospital would be left with zero reimbursement for medically necessary services. Importantly, this improvement *only* applies to claims that are submitted within 3 months of the date of service.

Limiting RACs to 30 days to complete complex reviews

RACs historically were required to notify providers within 60 days of the outcome of

complex reviews. Accordingly, if RACs adhere to the new 30-day timeframe, providers should receive feedback and be able to implement necessary compliance enhancements more rapidly. CMS's enforcement of this deadline, which has not yet been specified, will be crucial. Currently, if a RAC misses a deadline for completing the review, the RACs are still permitted to move forward with their review. This can be frustrating for providers who see this as a double standard, because providers are held to their filing deadlines. For example, if a provider fails to provide requested documentation within the applicable deadline, the claims will often be denied.

30-day wait before sending a claim to a Medicare Administrative Contractor for adjustment

RACs will be required to wait 30 days before sending a claim to a Medicare Administrative Contractor (MAC) for adjustment to allow time for a discussion request. The discussion period was designed to allow providers and RACs an opportunity to discuss and potentially resolve disputed claims without the expense and burden of the formal appeals process. However, in the past, RACs have quickly referred their findings to the MACs, meaning that overpayment determinations and repayment demands were made during the discussion period. Providers, in turn, would promptly file an appeal in order to meet the 30-day filing deadline and to avoid recoupment. Once the provider filed an appeal, RACs were required to stop the discussion period. In sum, because RACs could immediately initiate the determination process, the discussion period has not been as beneficial as intended and, in effect, providers were forced to choose between participating in the discussion period (which may or may not be useful) and filing an appeal to avoid immediate recoupment. With CMS's new enhancement, providers should be able to more easily pursue both the discussion period and a timely appeal to avoid recoupment.

Quality and accuracy enhancements

RAC contingency fees will be paid only after the second level of appeal is exhausted

Historically, RACs were paid their contingency fee immediately after recoupment of a denied claim, even if the provider pursued an appeal. CMS's program change, to pay RAC contingency fees only after the second level of appeal is exhausted, is intended to help incentivize RACs to make accurate decisions that can withstand the appeals process. While this is a step in the right direction, it may not be enough to adjust RAC behavior. Generally, the first and second levels of appeal are viewed as "rubber stamps" of the RAC decision. Providers view the third level, the Administrative Law Judge (ALJ) phase, as the first meaningful opportunity for review. This change may impact RAC behavior to a certain extent, but delaying RAC payment until after the third level would likely lead to more significant change.

This change may impact RAC behavior to a certain extent, but delaying RAC payment until after the third level would likely lead to more significant change.

Maintaining an overturn rate of less than 10% at the first level of appeal

CMS will require RACs to maintain an overturn rate of less than 10% at the first level of appeal, excluding claims that were denied due to no or insufficient documentation, and

claims that were corrected during the appeal process. CMS has stated that RACs who do not comply with this requirement will be placed on a corrective action plan that could include decreasing ADR limits or temporary restrictions on certain types of reviews. However, this requirement will likely not impact RAC behavior, because RACs currently maintain an overturn rate of less than 10% at the first level of appeal. As noted, the first level of appeal, redetermination by the MAC, is generally thought of as a "rubber stamp" and not as a meaningful review of the RAC decision. Indeed, as reported in the Fiscal Year (FY) 2013 RAC Report to Congress, Part A claims were overturned at only 7.6% at the first level of appeal.[9] Thus, the way this enhancement is designed is not likely to make a significant impact. Some providers could view CMS's selection of the 10% threshold, which is already satisfied, as an indication that CMS is already content with the RACs' performance.

Requiring RACs to maintain an accuracy rate of at least 95%

RACs that fail to meet the requirement to maintain an accuracy rate of at least 95%, as determined by validation contractors, will be subject to a progressive reduction in ADR limits. Again, however, most RACs already meet this standard. In FY 2013, three of the four RACs had accuracy rates well over 95%, with only one RAC falling below 95% to 92.8%.[10] Moreover, the standards validation contractors use to validate RAC performance are not publicly available, and the results of the validation contractor reviews do not comport with other measures.

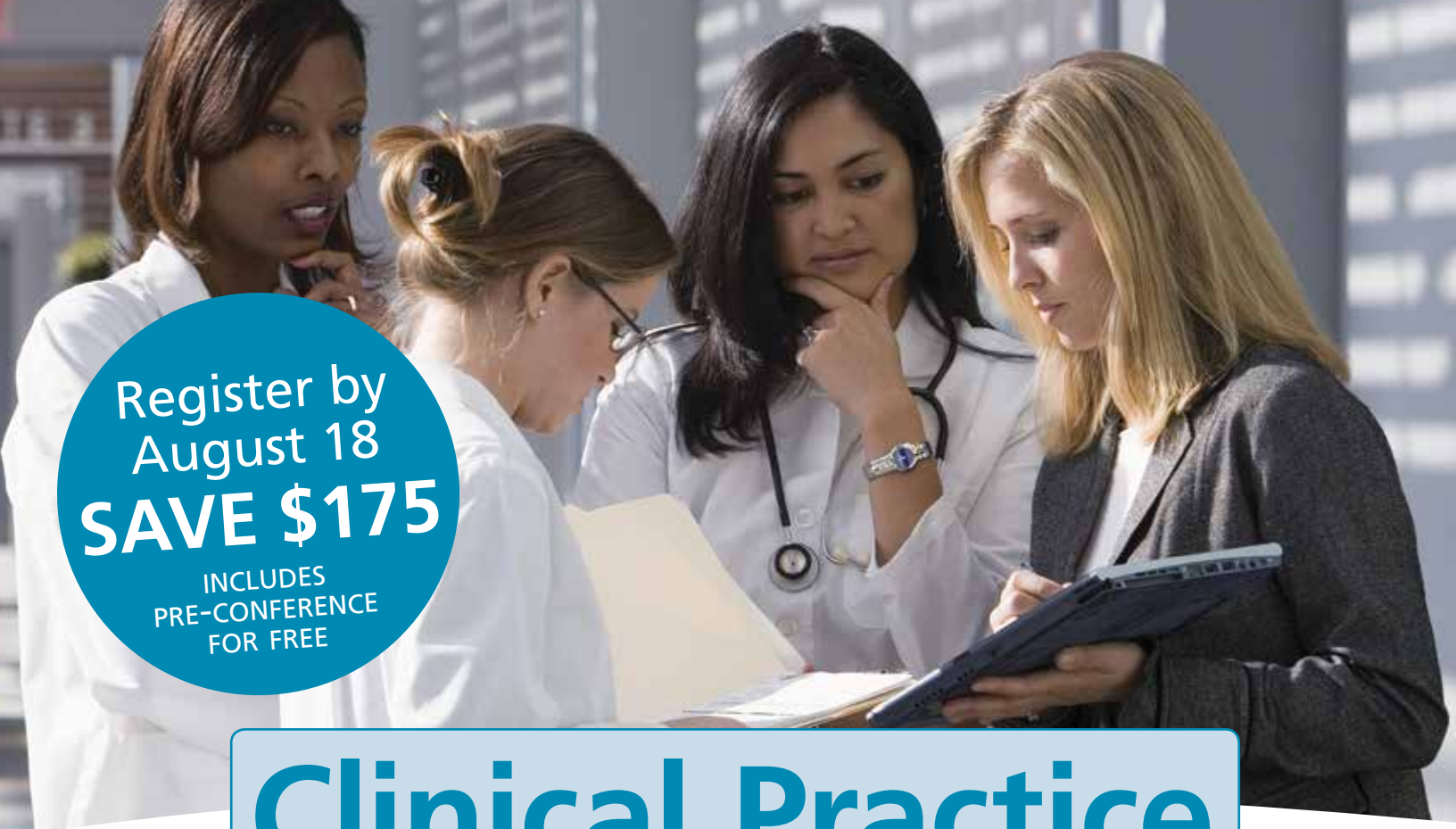
Conclusion and recommendations

The RAC program has recently garnered national attention because of the tremendous appeals backlog. CMS's efforts to reform the RAC program are undoubtedly a step in the

right direction. However, the practical significance of the program enhancements will be driven by the establishment of specific standards by CMS, as well as CMS's ability to enforce the program changes. Moreover, additional, more substantial reforms to the RAC program are needed to fully address the explosion of RAC denials and the resulting appeals backlog. Such reforms could take several forms, such as linking RAC payments to their overturn rates, delaying the payment of the RAC contingency fee until after the third level of review, or establishing an ombudsman to, among other things, enforce RAC compliance with these new contract provisions. Hopefully, there will be more program enhancements to come. To stay abreast of RAC program developments, providers should consider frequently visiting the CMS RAC page to monitor updates.

Finally, providers should not be lulled into a false sense of security by the reduction in RAC activity as a result of the Probe & Educate period and new contract delays. This may very well be the eye of the storm. Indeed, providers may want to prepare their organizations for the uptick in RAC reviews, including patient status reviews, which will come once the new RAC contracts are awarded.

1. See *Hearing on Exploring Medicare Appeal Reform Before the Committee on Oversight & Government Reform July 10, 2014* (statement of Nancy Griswold, Chief Administrative Law Judge, Office of Medicare Hearings and Appeals, Department of Health and Human Services). Available at http://1.usa.gov/1GjwAmS
2. *CGI Federal Inc. v. United States*, 1:14-cv-00355-MCW, Dkt. No. 53 (Fed. Cl. Sept. 3, 2014).
3. CMS: *Recovery Audit Program Recent Updates.* Available at http://go.cms.gov/1S1Fx8Q
4. Ibid.
5. Ibid.
6. CMS: *Recovery Auditing in Medicare for FY 2013.* Available at http://bit.ly/1yTWX4u
7. CMS: *Recovery Audit Program Improvements.* Available at http://go.cms.gov/1HcB3nq
8. Idem, endnote #3.
9. Idem, endnote #6.
10. Idem, endnote #6.



Register by August 18
SAVE $175
INCLUDES PRE-CONFERENCE FOR FREE

Clinical Practice Compliance Conference

OCTOBER 11–13, 2015 | PHILADELPHIA, PA

HOT TOPICS INCLUDE

- Coding Reviews and Education for Physicians: Turn their Dread into Delight!
- HIPAA Risk Management Programs: Doable, Practical, Financially Feasible
- Is Your EMR System Protecting the Rights of Your Adolescent Patients?
- Medical Necessity: Avoid Costly Audits
- Provider Risk In ICD-10: Justification through Appropriate Documentation
- Risky Business: Compliance Risks Associated with Electronic Medical Records (EMRs)
- Sampling 101: A Primer for Internal and External Audits
- Security Risk Assessment for Small Practices: Tools and Case Studies
- Drug Diversion by Healthcare Personnel: Essential Compliance Considerations
- Fundamentals of Physician Coding for Non-Coders
- "Incident To" and "Shared/Split BIlling": Are Your Providers Billing These Services Correctly?"
- Is Your Practice a Government Target? Pre-Audit Risk Assessment
- Physician Arrangements: Strategies to Reduce Compliance Risk
- The Art of Internal Investigations and Self-Disclosures
- The Compliance Officer's Role in Physician Contracting
- The OIG Self-Disclosure Protocol and Statistical Sampling for Non-Statisticians
- Using CERT Data to Fine Tune Your Audits

Learn more at hcca-info.org/clinical

Questions: catherine.stollenwerk@corporatecompliance.org

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

by David Hoffman, JD, FCPP

Diabetes care and monitoring—What works?

David Hoffman *(dhoffman@DHoffmanAssoc.com) is President of David Hoffman & Associates, PC, a national healthcare consulting firm in Philadelphia.*

Years ago, I settled a case that involved, in part, the failure of a nursing home to provide adequate care to residents who had diabetes. A major cause of these failures stemmed from the lack of appropriate monitoring of blood sugars. I worked closely with an expert, Stanley M. Schwartz, MD, in developing a blood sugar monitoring tool to address hypo- and hyperglycemia. Recently, I was in a facility that was still using sliding scale insulin and the residents' blood sugar levels appeared to not be well controlled. This led me back to check in with Dr. Schwartz and he advised me that:

Hoffman

1. Significantly nursing homes were not monitoring fingerstick sugars in patients on sulfonylureas and glinides, and were insufficiently monitoring those taking insulin.
2. There is now much published data on the risk of sulfonylureas: increasing adverse cardiovascular outcomes and death after being on sulfonylureas for one year 1.8x, and 2.5x one year after starting insulin.
3. We know patients >65 years of age, in any setting, have more visits to ERs and admission to the hospital for hypoglycemia than hyperglycemia.
4. Regulatory commissions agree a "new sulfonylurea" agent would not pass current FDA or European Medicines Agency guidelines for cardiovascular safety if brought before them for approval.
5. Most importantly, we now have agents that can control sugar, in many cases at the same site sulfonylureas act, but without causing hypoglycemia. In addition, we have agents that work as quickly as insulin, preserving beta-cell function, but without its attendant weight gain and hypoglycemic risk.

> Thus, [he] advocates a "ban" on the use of sulfonylureas in everyone, but especially in the elderly.

Thus, Dr. Schwartz advocates a "ban" on the use of sulfonylureas in everyone, but especially in the elderly. He would use three or four non-insulin, non-hypoglycemic agents before considering insulin therapy and would continue them if there is a need to start basal insulin. This approach would obviate the need for meal time bolus insulin in most (which is often given as sliding scale), which would reduce the risk of hypoglycemia with insulin therapy by 85%.

In conclusion, it is apparent that monitoring of patients/residents with diabetes who require medication is essential from a quality-of-care perspective. Importantly, the compliance officer should take a proactive role in requesting that the medical director review the current medical management of patients with diabetes and whether your facility's approach constitutes "best practice." This clinical issue implicates compliance concerns around quality of care based on current medical literature.

SCCE Regional Conferences

Network & learn locally and earn CEUs

Join us in 2015 to share information about compliance successes and challenges, enjoy an inexpensive educational opportunity close to home, and earn CEUs.

Questions? jennie.nguyen@corporatecompliance.org

Don't miss your chance to register for one of SCCE's four remaining 2015 Regional Conferences

October 23, 2015
Minneapolis, MN

November 13, 2015
Boston, MA

October 30, 2015
Atlanta, GA

December 4, 2015
Dallas, TX

corporatecompliance.org/regionals

by Shelly L. Harris, RHIT, CHC, CHPC, CCS

Compliance tips: Evaluate your effectiveness by asking 50 questions

» Build awareness and effectiveness by asking the right questions.
» Apply the answers to the annual risk assessment and work plan.
» Create metrics based on questions.
» Assess the tone and climate of an organization.
» Completing a small employee survey can help evaluate effectiveness.

Shelly L. Harris *(Shelly.Harris@Altegrahealth.com) is Senior Consultant at Altegra Health Operating Company. Shelly is based in New York.* bit.ly/in-ShellyHarris

Are you an effective compliance officer? As the compliance officer, what are you doing to ensure the organization is compliant with state and federal regulations? Are employees educated about the most important compliance requirements? Have compliance surveys been conducted in the past? Are you, as the compliance officer, visible and available to staff at all levels within the organization? Do the surveys inquire about the organizational and staff compliance and ethics questions? Are surveys used for this purpose annually at all?

Harris

When doing in-person interviews and walk-through of the various areas within the facility and business areas, define definite points to observe, watch, and listen. All this information will be used to evaluate compliance program effectiveness and how those responses and actions play into the culture of compliance within the organization.

These common questions face compliance officers in almost every industry worldwide. Building an awareness of compliance regulations and ethical business standards is the best approach to validating the program and the effectiveness of a compliance officer. Once the objective and subjective answers have been categorized, use the information to develop an assessment to support the items included within the draft work plan. The draft can provide metrics that the board and senior management can use to consider projects, to justify audits and assessments, or to provide a more detailed evaluation once deficiencies are identified, and where the most important improvements can be made.

Policies and procedures

A great place to start the evaluation of compliance effectiveness is with the corporate compliance policies, procedures, and code of conduct. Once you have identified the location and obtained the relevant documents, consider some of these questions:

- Are compliance expectations clearly documented?
- Are the organization's policies updated?
- Are there any apparent gaps compared with the OIG model compliance plan most applicable to the organization and each department?

- Could the up-to-date compliance plan, code of conduct, and policies and procedures produce up-to-date policies if a federal or state auditor requested them?
- Do the employees in the organization have access to and know where to find the policies?
- Has your code of conduct been revised and approved by your governing body?

Another first step would be to inquire with Human Resources (an integral part of Compliance) and ask for a sample number of employee records (15–30) to audit. Check the records to verify that the sample employee records have written verification noting receipt of the code of conduct and/or an acknowledgment form that employees know how to access an electronic copy. In addition to the code of conduct, do the employee records verify completion of their initial and annual compliance training?

Assess the tone/culture at the top

Ah, yes, that ethical atmosphere in the workplace and the culture at the top trickling down to the employees. Culture drives employees to believe or not believe in an organization. Can tone make a difference in culture? In a word, yes! The cultural tone has the ability to drive morale, productivity, loyalty, and trust. Staff spend countless hours at work, so it is essential to engage employees and drive an ethical culture. Education and training will encourage employees to report situations they learned about in compliance training. Compliance should oversee the climate of the organization with fairness and due diligence, and must enforce the code of conduct and discipline employees who don't live up to company standards. Compliance has become the highway that bridges crucial dialogue between employees, senior management, and the board. This sends the message to employees that the organization is serious about listening, and a compliance professional is present to assist when reporting difficult situations. Compliance professionals should consider asking the following questions to gage their position in setting the tone at the top:

- Does the compliance officer interact regularly with senior management?
- Does the compliance officer report to the board or governing body?
- Does the compliance officer provide education to the chief executive officer (CEO) and his/her senior management team?
- Is education provided to the board and employed providers?
- Is the compliance officer involved in investigations and interviews when issues arise (e.g., patient care and business quality)?
- Does the tone at the top reflect a high level of integrity for others to follow?
- Is the compliance officer privy to conversations regarding revenue enhancement changes that are being made?
- Are the board members and senior management engaged?

> Can tone make a difference in culture? In a word, yes!

If some of these answers are no, try requesting face-to-face time with leaders in the organization. Provide documentation about compliance best practices and include language from the Federal Sentencing Guidelines, Chapter 8. Be the facilitator, the negotiator, or the person presenting the ideas to influence positive change.

Training and education

There are several ways to evaluate the effectiveness of your education and training. Start by asking more questions and documenting the responses. Evaluating the education and

training that new employees are receiving, as well as reviewing the annual compliance training, can suggest some areas that may need additional compliance guidance. Some important considerations would be:

- Is the compliance officer personally involved in training?
- Does the subject-matter expert, the compliance officer, or their designee, teach the training?
- Does the compliance officer have input regarding what information will be included in new employee and annual employee training programs?
- Is the compliance officer appropriately engaged and does he/she interact with the staff?
- Does the compliance officer ensure confidentiality and is he/she trusted by the employees?

Being knowledgeable about the compliance training program can aid in the efforts toward effectiveness and awareness. By utilizing the education platform, awareness can be increased just by disseminating information. Business cards can be distributed at new employee orientation. Emails can be used to send reminders about compliance activity or include quizzes that reward the first correct responders. Quarterly newsletters are still effective. Any or all of these can be used to enhance the awareness of the program, and get the compliance officer's presence, identity, or how to report non-compliance front and center.

Active monitoring and auditing efforts

While in a recent role as a compliance officer, I recall two instances in the course of a review that a state auditor and a government official asked: "Has your organization self-disclosed? How many times?" These are great questions to consider as you evaluate the current active monitoring and auditing taking place.

No one's perfect. Review the organization's Compliance department list of historical investigations:

- Are there any instances where you have or you should have self-disclosed?
- Were the efforts to identify the magnitude of an issue enough to verify that the correct disclosure was made?
- Is there a self-disclosure process and return of overpayments built into department operations?
- Are there any internal controls built into the system? What are they?
- Were internal controls and the documentation of the issue sufficient to gain an understanding of the problem and was corrective action put in place to rectify the situation?

In addition to auditing and monitoring, compliance officers should evaluate other practices, such as business development. Hopefully, the focus is not solely on making a profit rather than following the rules and regulations.

Conducting employee surveys

One of the best ways to evaluate the effectiveness of a compliance program is to conduct an employee survey. The survey need not be all inclusive; a small random sampling of the employee population will suffice. The use of Internet-based survey programs is appropriate if an organization does not have one internally. Choose 20 staff at random and send them an email, or pick up the phone and ask more questions!

- Who is the compliance officer?
- What's the Compliance and Privacy hotline number?
- Who do you call when you need to report a concern?
- Do you know where to find the organization's code of conduct and do you know what it means?

Unfortunately, when asking these questions, the compliance officer or designee may find many employees don't really know the answers. It is the compliance officer's responsibility to influence the change needed to increase the employees' awareness and understanding of the information and their obligations under the organization's compliance plan.

Addressing issues and tracking information

When complaints are received, it is paramount to remain objective and really listen to the complainant. A well-documented investigation adds to the detail required when a concern is reported. So, listen, address, document, and track.

Have you ever wondered why the Compliance hotline doesn't ring?

- Is it working? (Not everyone has an outsourced mechanism to track complaints.)
- Was there a power outage and now it's not working properly? Have you randomly tested it?
- Is there a log for Compliance and/or Privacy hotline calls?
- Is there a mechanism or file system used to investigate and document issues?
- Are complaints and concerns tracked, categorized, and investigated in a timely manner?

A compliance officer must have strong leadership competencies and a high level of integrity. Compliance officers are mandated to encourage others to report compliance violations and unethical business practices, and adhere to company and department-specific policies. It is also the compliance officer's responsibility to validate audits and follow through on reported activities of non-compliance.

Strong leadership skills and business acumen can guide compliance officers who are in the trenches, caught between being the mediator and implementing the rules and regulations. Interpreting compliance regulations and informing senior management and the board of directors is one of the primary responsibilities of a compliance officer. In addition, the compliance officer is expected to influence and persuade senior and middle managers to change processes and self-disclose problems, when necessary and appropriate. Of course, the interpretation and influence from the compliance officer is based upon the individual's knowledge, experiences, education, and, in some instances, instinct.

Whistleblower cases, lawsuits and settlements, allegations of corporate fraud, and various other instances of non-compliance are continually making national and global news. Does the organization have the ability to make tough decisions and be a dynamic industry leader? Does the organization support doing the right thing or look in the opposite direction when faced with difficult compliance situations? These aren't easy questions to answer. But, there is a place to begin. Make a difference by using some of these tips to help ensure your program is headed in the right direction to avoid costly mistakes.

Being an effective compliance officer requires more than honesty and integrity. It necessitates a determination to investigate and follow through. It is the compliance officer's responsibility to take action.

1. OIG Supplemental Compliance Program Guidance for Hospitals: 70 fed. Reg. 4858. January 31, 2005 (amending 63 FR 8987, issued February 23, 1998).
2. False Claims Act, 31 U.S.C. §§3729-3733
3. United States Sentencing Commission: Federal Sentencing Guidelines, Chapter Eight, Sentencing of Organizations §8B2.1. Effective Compliance and Ethics Program.
4. State of New York, Office of the Medicaid Inspector General: Bureau of Compliance Identified Compliance Program Best Practices, March 31, 2014. Available at http://bit.ly/1rReii ; and Identified Program Insufficiencies as of June 30, 2014. Available at http://on.ny.gov/1cLglTE
5. New York State Social Services Law, §363-d subd. 2 and 18 NYCRR 521.3(c). PowerPoint, OMIG's New Compliance Program Assessment Form and How the Compliance Program Review Function Operates. November 14, 2012. NYS SSL §363-d subd. 2 and 18 NYCRR 521.3(c). Available at http://on.ny.gov/1SbvGws

by Janice Anderson and Sara Iams

The Two-Midnight Rule: Past, present, and future *[UPDATE]*

» The Two-Midnight Rule is highly controversial and its future is questionable.

» Since the adoption of the Two-Midnight Rule, CMS enacted a Probe & Educate program and delayed RAC enforcement of the Two-Midnight Rule, in large part due to push-back from the industry.

» The deadline that would trigger RAC enforcement of the Two-Midnight Rule has been extended several times, most recently through September 30, 2015.

» The Medicare Payment Advisory Commission (MedPAC) also is not favorable to the Two-Midnight Rule and recommended withdrawal of the Rule.

» In the 2016 proposed Inpatient Prospective Payment System (IPPS) rule, CMS indicated that it would consider the MedPAC recommendations in its rule-making related to the 2016 proposed Outpatient Prospective Payment System rule to be released this summer.

Janice Anderson *(janderson@polsinelli.com) is a Shareholder in the Chicago office and* ***Sara Iams*** *(siams@polsinelli.com) is an Associate in the Washington DC office of Polsinelli PC.* /in/saraiams

This is an update to the article entitled "The Two-Midnight Rule: Past, present, and future," published in the May 2015 edition of *Compliance Today*. Since the adoption of the Two-Midnight Rule, CMS has repeatedly extended the Probe & Educate program and delayed RAC enforcement of the Two-Midnight Rule, in large part due to push-back from the industry. At the time of the original article, CMS had recently moved the deadline to April 30, 2015, and Congress was in the midst of debate on whether to further extend it.

Two new developments have occurred since the article was published. First, on April 17, with the passage of the Medicare Access and CHIP Reauthorization Act of 2015, Congress once again authorized CMS to extend the Probe & Educate program through September 30, 2015 and barred RACs from conducting post-payment reviews for hospital discharges occurring through September 30, 2015, other than in instances of suspected fraud. It's not clear whether this will be the final delay or whether Congress or CMS will intervene once more as September approaches.

Anderson

Iams

Second, although CMS declined to provide specific guidance, it announced in the 2016 Inpatient Prospective Payment System (IPPS) proposed rule that it would consider feedback from the Medicare Payment Advisory Commission (MedPAC) regarding the Two-Midnight Rule. In its June 2015 *Report to the Congress*, MedPAC made several recommendations, most notably that CMS should withdraw the Two-Midnight Rule altogether and should direct RACs to focus reviews on those hospitals that have the highest number of short inpatient stays. According to the 2016 IPPS proposed rule, CMS will address the MedPAC recommendations more thoroughly in the 2016 Outpatient Prospective Payment System (OPPS) proposed rule, due to be released this summer.

The Society of Corporate Compliance & Ethics 14th Annual

Compliance & Ethics Institute

October 4–7, 2015
ARIA in Las Vegas
Las Vegas, NV

GENERAL SESSION SPEAKERS ANNOUNCED

Marjorie W. Doyle
Marjorie Doyle & Associates, LLC

Debbie Troklus
Managing Director, Aegis Compliance and Ethics Center

Odell Guyton
Vice President, Global Compliance, Jabil Circuit, Inc.

Art Weiss
Chief Compliance & Ethics Officer, TAMKO Building Products

Dr. Garrett Reisman
STS-132; Crewmember, International Space Station

Kelly R. Welsh
General Counsel, U.S. Department of Commerce

Learn more and register at ***complianceethicsinstitute.org***

Questions?: *Lizza.catalano@corporatecompliance.org*

by Kelly M. Willenberg, MBA, BSN, CHRC, CHC, CCRP

Medicare Secondary Payer obligations for sponsor

Kelly M. Willenberg *(Kelly@kellywillenberg.com) is President and CEO of Kelly Willenberg, LLC in Chesnee, SC.*

As more pharmaceutical companies are reporting injuries arising from clinical trials that involve Medicare beneficiaries, the industry is adjusting and trial sites are becoming more accustomed to fulfilling requests for test subjects' personal information.

Willenberg

Section 111 of the Medicare, Medicaid and SCHIP Extension Act (MMSEA) of 2007 requires trial sponsors to: (1) determine whether an injured party is entitled to Medicare benefits; and if they are, then (2) they must report their acceptance of their responsibility to make ongoing medical payments related to treating the injury. Although the penalties for not reporting are heavier than the Sunshine Act ($1,000 per day per unreported beneficiary), implementation costs are much lower, and the actual fiscal responsibility taken on by the sponsor can be controlled. For instance, sponsors generally adjudicate the injuries reported by the sites by only considering related adverse events and then only those events that were not the fault of the test subject, failure to follow protocol, etc., as dictated by their clinical trial agreement with the site.

Actually, collecting the patient personal data required to be reported may be the hardest part of reporting. The conflict arises when Medicare wants to know who suffered the injury and sponsors don't want to destroy the double-blind nature of the test by collecting that information. Sponsors generally hire a Section 111 Reporting Agent to act on their behalf. Sponsors provide non-identifying information to the agent (e.g., study ID, site ID, patient ID) and then the agent contacts the site to collect the first name, last name, DOB, gender, and Social Security number of the test subjects. Site personnel have been trained to protect that information, so agents spend a lot of time reassuring the site that the disclosure is legal and warranted. Medicare recently made that easier by requiring only the last five digits of the Social Security number in order to determine if a test subject is enrolled in Medicare.

The conflict arises when Medicare wants to know who suffered the injury and sponsors don't want to destroy the double-blind nature of the test…

In an interview, David Piatt of Medicare Consul Services said, "Pharmas are adding language to their CTAs [clinical trial agreements] requiring sites to support Section 111 collection efforts and, after contacting thousands of sites, I can say the word is spreading. Clinical sites are tuning in and becoming more cooperative."

Despite Medical secondary payers' checkered history, CMS issued formal guidance in their Non-Group Health Plan (NGHP) User Guide, backed by hefty penalties. Sponsors are stepping up their efforts to comply, and sites are getting on board.

PLAN NOW TO CELEBRATE IN 2015

Corporate Compliance & Ethics Week
November 1–7, 2015

NEW DATES IN 2015

Official Poster
20"× 28" glossy color poster
$6.25 ea. (min. order 5)

Table Tents (8-pack)
Pre-cut, 4"×6" two-sided cardstock tents with 8 different questions to get your employees thinking about compliance. Visit hcca-info.org/CandEweek for a list of the questions.
$2.50/8-pack (min. order 10)

Break-Resistant Mug
14 oz. translucent acrylic mug made of durable and chip-resistant material.
$4.25 ea. (min. order 5)

Sticky Note Caddy with Flags
Features 3 different sizes of sticky notes with 5 assorted colors of flags.
$2.50 ea. (min. order 10)

Microfiber Lens Cloth
A 6" x 6" cloth that lifts dust and oils from electronic screens or eyeglasses without chemicals. Includes holding pouch.
$1.00 ea. (min. order 25)

Earbuds in Triangular Case
Includes 46" cord and protective case. Encourage a speak-up culture with the words "WE'RE LISTENING."
$4.00 ea. (min. order 5)

Silicone Awareness Bracelet
Let everyone know: "WE'RE LISTENING."
$0.50 ea. (min. order 50)

Bic Fusion Highlighter
Strong and durable plastic body matches the highlighter's ink color.
$1.25 ea. (min. order 25)

Touch Point Light-Up Pen
Features a ballpoint pen, flashlight, and touch-point tip/stylus to use on standard electronic devices.
$3.00 ea. (min. order 10)

NOVEMBER 1-7, 2015
CORPORATE COMPLIANCE & ETHICS WEEK
WE'RE LISTENING

Join organizations worldwide in championing workplace compliance and ethics

ORDER DEADLINE: OCTOBER 1, 2015

corporatecompliance.org/CandEWeek *or* hcca-info.org/CandEWeek

by Nadia Fahim-Koster, CISSP, HCISPP

Whip your incident response program into shape

» Understand requirements behind an incident response program (IRP).
» Identify the different components of an effective IRP.
» Learn how to prepare for your testing exercise.
» Learn how to develop meaningful testing scenarios.
» Understand how to conduct and document the testing.

Nadia Fahim-Koster *(nadia.fahim-koster@meditologyservices.com) is Director, IT Risk Management with Meditology Services, LLC in Atlanta.*
bit.ly/in-NadiaFahimKoster

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires covered entities to "identify and respond to suspected or known security incidents, as well as mitigate to the extent practicable, harmful effects of security incidents that are known to the covered entity, and document security incidents and their outcomes."[1]


Fahim-Koster

To comply with this standard, covered entities must develop a comprehensive incident response policy, as well as a plan that outlines the different steps that should be taken in the event of an incident. To be effective, incident response takes careful planning and practice. An incident response program (IRP) requires organization, training of key personnel, and systematic procedures. Several annual test exercises must also be conducted as a key requirement to ensuring your organization is ready in the event of an actual incident.[2]

You can test your IRP in many different ways. This article will provide you with some key elements that will help you put in place an exercise to test the effectiveness of your organization's security IRP.

Incident response program

An effective IRP includes a policy, a plan, and a set of procedures. The National Institute of Standards and Technology (NIST) has issued guidance for each of these steps.[3]

The policy

An IRP policy is the first step in establishing your program. The policy is used to affirm your organization's commitment to establishing an IRP. It outlines the scope of the program and the roles and responsibilities of the different stakeholders. The National Institute of Standards and Technology (NIST) recommends that the following elements be included in the IRP policy:

- Statement of management commitment;
- Purpose and objectives of the policy;
- Scope of the policy;
- Definition of security incidents and related terms;
- Roles, responsibilities, and levels of authority;
- Severity ratings of incidents;
- Performance indicators; and
- Reporting and contact forms.

The plan

Once your organization's IRP policy is defined and approved, the next step is to develop an IRP plan. The plan should be tailored to the size, structure, and mission of your organization. NIST recommends that the following elements be part of your IRP plan:

- Senior management sponsorship and approval;
- Goals and objectives for incident response;
- Organizational structure of the various team members, their resource requirements, and their roles;
- Communication process for internal and external entities;
- Outline of the incident response methods for each classified incident from the policy;
- Metrics for evaluating the effectiveness of the team and process; and
- Processes for annual review and evaluation.

The procedures

Finally, the last step in the IRP is the development of a set of procedures that document in sufficient detail all of the activities that must take place during each one of the five phases of an incident response—preparation, identification, containment, eradication, and recovery.

The most common procedures include the following elements:[4]

- Communication—both internal and external to your organization,
- Escalation notification,
- Incident tracking forms,
- Incident reporting and documentation
- Investigation checklists by technology platform,
- Remediation checklists by risk and threat classification,
- Security information event management (SIEM),
- Evidence collection and handling "chain of custody",
- Forensics investigation and documentation,
- Data retention and destruction, and
- Non-disclosure agreements.

Once all elements of an IRP are in place, it is ready to be tested. Testing is an integral piece of the overall program and is the only way to assess the effectiveness of the program. You do not want to wait until you're in the middle of a real-life incident to find any holes or weaknesses in the IRP.

Incident response testing preparation

Although there are many possible approaches to testing an incident response program, a tabletop exercise is the most cost-effective, non-threatening, and non-disruptive format to test your organization's ability to respond to an incident. It is a discussion-based exercise during which the team will discuss roles and responses for a particular scenario or situation. The exercise does not involve deploying equipment or other resources.

A tabletop exercise, just like any other testing exercise, also has its limitations. The test provides only a high-level estimate of the current potential for success of a cyber-security incident response plan. It also carries considerable uncertainty regarding the skills, available resources, and actual capabilities necessary for execution of the plan.

The objective of the tabletop exercise is to determine whether participants can realistically "talk through" their critical functions during an incident response scenario, and help participants become more aware of possible weaknesses and gaps in the incident response plan.

So, where to start?

A good IRP test requires adequate preparation. You first want to look at every component of your IRP, including a review of your IRP policy. Make adjustments where necessary to ensure that everything documented is accurate, and

assess your procedures documentation for potential improvements and/or changes.

The next step of the preparation is the creative part of the exercise, as the team develops different incident scenarios. It is important to identify the participants who are part of this exercise. The easiest way to do this is to review the IRP and identify the different teams listed within the document. Determine whether you will involve every member of every team, or just a representative. For instance, if your plan calls for the network team, you may only want to invite a single representative from that team to keep the exercise nimble and dynamic.

Next, identify the scenarios that will be used during the exercise. An effective way to go about completing this step is to take into consideration the different incident criticality levels as identified in the IRP plan. For example, if the criticality levels are critical, high, medium, and low, you might want to create scenarios for each category to assess how the teams respond to each level. For instance, responding to a major virus outbreak will be handled very differently than being notified that a laptop containing patient data was lost or stolen.

You can also create scenarios that align with real-life incidents in the industry. For example, a high-profile corporate breach can provide a nice example for a critical-level incident. You can design scenarios around stolen/lost laptops, PHI emailed to incorrect recipient(s), hacked medical devices, a defaced organization website, etc. The point is that the scenarios should be designed to not only align with IRP criticality levels, but also represent realistic and true-to-life occurrences.

The point is that the scenarios should be designed to not only align with IRP criticality levels, but also represent realistic and true-to-life occurrences.

Last but not least, one of the scenarios should test for the effectiveness of your organization's HIPAA Breach Notification plan. The HIPAA Breach Notification provision of the HITECH Act mandates that covered entities notify their patients and the Health and Human Services (HHS) Secretary in the event of a data breach. You should walk the team through a scenario involving the loss of patient data to see if they are able to comply with the required process, including the notification to patients, HHS, and the media (if the scenario is applicable).

Once participants have been identified and scenarios designed, a facilitator must be designated for the exercise. The facilitator's role is to help participants step through the exercise in an organized manner, ensure the active participation of all team members, raise difficult questions, make certain that the IRP is being followed, and verify that any identified issues are documented. To that end, the facilitator may need one or two scribes to assist with note taking in order to produce an accurate report at the end of the exercise.

Conducting the tabletop exercise

The day of the test has arrived, your participants have shown-up, your scribes are ready to go, and more importantly, you've remembered to order coffee, bagels, and donuts to keep the room well fed and engaged! You have also remembered to have several copies of your organization's IRP on hand.

As the facilitator, first outline your role and responsibilities during the course of the exercise. Then ask all members of the team to introduce themselves and the areas they

represent. Describe to the team what your organization intends to accomplish by conducting an IRP tabletop exercise. Explain what an example scenario looks like and how you will walk the participants through the incident. Lastly, don't forget to describe the role of the scribe(s). Be sure to encourage the scribe(s) to be vocal if they need the team to pause while they are taking notes or if they need clarification on any issues being discussed.

You are now ready to start the first scenario. Choose to begin with either a low-level incident or a critical-level incident. If you decide to start with a low-level incident, participants have time to warm up to the exercise and familiarize themselves with the format before addressing more complex critical-level incident(s). On the other hand, starting with a critical-level incident helps you to quickly gauge the participants' familiarity with the IRP and how they will manage in the event of a real incident. Either way, the point is for the participants to understand what their roles are with respect to the IRP and how they should react during a real incident.

Read the scenario to the team and give them a few minutes to digest the information before proceeding. To help illustrate, assume an example scenario describes the following incident:

> *In the post-surgical unit, all of the PCA (patient controlled analgesia) pumps suddenly start beeping. The nurses report that all the settings have been wiped out and every pump has been rendered dysfunctional. There were five PCA pumps in the unit at the time. The charge nurse has been notified.*

As the facilitator, you can help the team get started by asking them some questions such as:

- How would you handle this incident?
- Who should the charge nurse notify?
- Would she notify the IT Service Desk or would she call the Biomed department?

> There are no right or wrong answers… The point of the exercise is to ensure that your organization's IRP is being followed as closely as possible and that any issues are identified.

Once the conversations have started, you will need to continue to help steer the team in the right direction. There are no right or wrong answers as to how an incident is ultimately handled. The point of the exercise is to ensure that your organization's IRP is being followed as closely as possible and that any issues are identified.

As the team starts analyzing the different possibilities and outcomes, make sure they adhere to the IRP documents and that they are able to follow the documented process. Whenever the team is unable to progress to the next step due to missing information or procedures, ensure the scribes capture these findings.

Occasionally the team will miss a nuance that was specifically included in the scenario, or will not arrive at a particular intended outcome (e.g., a scenario where medical devices have stopped functioning should lead the team to realize that the Biomed department should be notified). In these circumstances, it is the facilitator's responsibility to ask the questions that will lead the team to come to the correct conclusion.

At the end of the first exercise, be sure to summarize the events, run through the list of "to-dos'" identified by the team

during the exercise, and perform a "lessons learned" session.

The second scenario should introduce unexpected variables during the course of the exercise, to throw the team off guard and see how they handle new, unexpected information.

Documentation of the incident response tabletop exercise

Writing the report is probably the most difficult part of the tabletop exercise. The challenge is to present a large volume of information in a manner that is easily read and understood.

There are many different ways to document the report. Ensure the scenarios are described and include all the notes for each scenario, including candid conversations. The report should include takeaways and a to-do list, as well as all associated notes. This allows those individuals responsible for updating the plan to reference specific notes from the conversations during the IRP update process. The report is evidence that not only does your organization have an IRP, but that the IRP has been tested. Keep it handy for the next time you conduct a tabletop exercise, because you will need it to verify that any required updates were made.

Conclusion

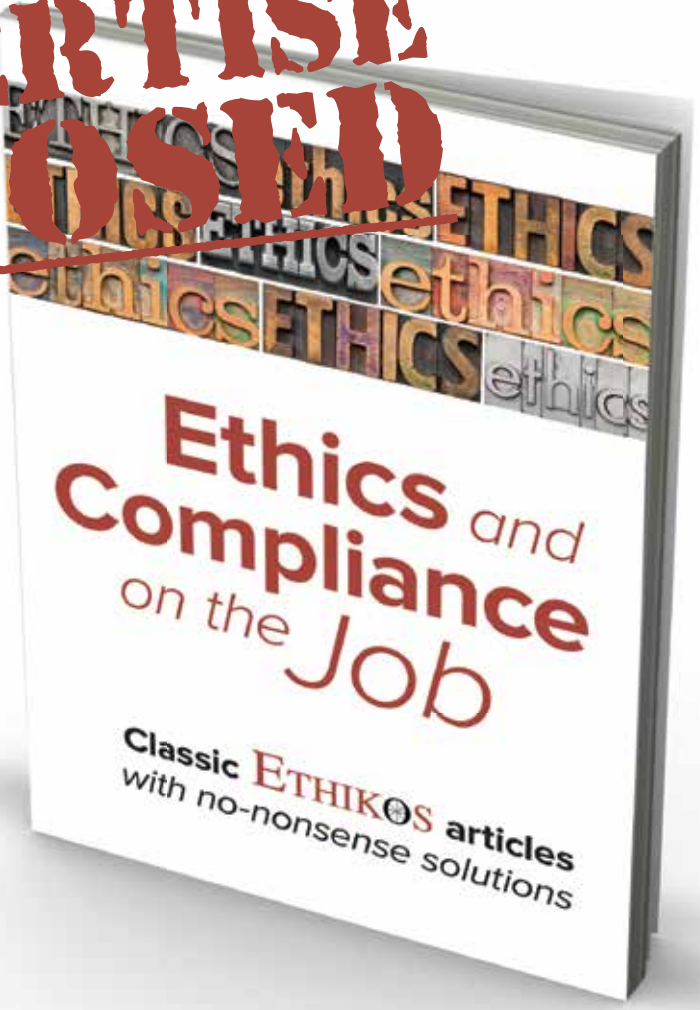
Many organizations have an incident response program in place, but many do not test the program on a regular basis. Testing an IRP is no guarantee that you will be able to handle an incident without any glitches, but it will make handling real-life incidents more effective and more efficient.

1. Department of Health & Human Services: HIPAA Security Series:Requirement 164.308(a)(6)(i) – Response and Reporting. Available at http://1.usa.gov/1JX9Xn8
2. Kurtis Holland: "Incident Response Exercise Planning Be Ready – Be Prepared." SANS Institute Reading Room, April 7, 2014. Available at http://bit.ly/1cMUMC2
3. NIST Special Publication 800-61, Revision 2 – Computer Security Incident Handling Guide
4. Idem, ref #2.

For 27 years, ethics and compliance experts have gathered to share ideas in the pages of Ethikos.

Here's your chance to see why.

EXPERTISE EXPOSED



Now available from HCCA.

Visit www.hcca-info.org/EthikosBook
or call 952-405-7900 or 888-580-8373

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

by Virginia Sizemore, CHC, CIA, MBA and Chris Luoma

Decreasing the chances of extensive, costly OCR audits

» All hospitals must now have business associate (BA) agreements in place.
» Hospitals with multiple violations could face $6 million in fines.
» The first step is understanding the risks represented by BAs.
» Every company paid within past 24 months should be examined.
» If audited, hospitals should send only the information requested.

Virginia Sizemore *(vsizemore@windstream.net) is a healthcare administration professional with over 26 years of experience in the field and lives in Decatur, GA.*
Chris Luoma *(cluoma@ghx.com) is Vice President, GHX in Atlanta.*
bit.ly/in-VirginiaSizemore *bit.ly/in-ChrisLuoma*

With increased audit volumes and higher fines for data breaches, it's not surprising that hospital compliance leaders feel they're playing against a stacked deck. The Omnibus deadline has passed—all business associates (BAs) must have been identified and have signed an updated business associate agreement (BAA) by now—and hospital risks now extend to those BAs.

Hospitals are receiving Health and Human Services Office of Civil Rights (OCR) audit notices, and the stakes are high—each fine for willful neglect without correction costs $50,000. The fines are limited by category to a maximum of $1.5 million, but a hospital with multiple violations in each of the four violation categories within a calendar year could face up to $6 million in fines. The personal health information (PHI) breaches, reported almost daily, are similarly pricey. The average cost to an organization of a breach is $2 million, but that rises to an average of $8.7 million for any breach involving more than 500 records.

Fortunately, hospitals are not up against a Las Vegas casino. By acting now to fully understand the risks posed by BAs and taking steps to mitigate them, compliance leaders can improve the odds they'll come through an audit with only modest penalties related to BAs—or none at all.


Sizemore


Luoma

Four mitigation steps

The first step to mitigation is understanding the true risk represented by BAs. Not only do hospitals have nowhere near the control over BAs that they have over their own departments, but BAs are disproportionately risky. Although BA breaches represented 41% of 2014 breaches,[1] they impacted 62% of patient records.[2]

Beyond the financial risk of a BA breach lies another risk: damaging a hospital's reputation. If a hospital's vendor's subcontractor fails in its duty to protect patient PHI, the story will likely appear somewhere around page 20 of the local newspaper. In contrast, the affected hospital responsible for a HIPAA breach caused by a BA is sure to appear in a page-one article, potentially damaging its reputation with their entire stakeholder roster: patients, self-insured employers, payers, providers, risk assessors, and the community.

Mitigation 1:
Identify all BAs

This step is more complicated than in the past, thanks to the expanded BA definition. Examples of new categories of BAs include: patient safety organizations, health information organizations, data storage companies, entities that offer personal health records, and subcontractors that maintain or transmit PHI on behalf of another BA. In one instance, a janitorial service was determined to be a BA, because it was involved with shredding documents containing PHI.

Hospitals need a cross-functional team that includes personnel from Procurement, Revenue Cycle Management, Compliance, Internal Audit, Operations, and IT. The team must be headed by someone with the responsibility and authority needed to motivate a multidisciplinary team and engage with high-level leaders.

The team should begin the vetting process by examining the BA status of every company the hospital has paid within the last 24 months. It should create a common vendor master across all parts of the organization, especially if the organization recently acquired or merged with another entity.

Mitigation 2:
Document BA oversight

The team should also prepare for an OCR audit or other HIPAA-related investigation by carefully documenting policies and processes supporting BA oversight. It should be prepared to show, at minimum:

- A list of BAs with updated contact information and category,
- A rubric that explains vendor categorizations,
- Proof of signed agreements with all BAs,
- Copies of all HIPAA policies and procedures,
- Proof that all employees have been provided with HIPAA training and security reminders,
- A copy of the most recent security risk assessment, and
- A copy of the incident response plan.

Mitigation 3:
Examine vendors for non-BA issues

Several other issues should be part of the vendor onboarding/vetting process, including:

- **Checking the OIG list.** OIG maintains the List of Excluded Individuals and Entities (LEIE) on its website (*http://oig.hhs.gov/exclusions*), which contains OIG program exclusion information. To avoid potential civil monetary penalty (CMP) liability, providers should check the LEIE prior to employing an individual or contracting with a contractor. OIG updates the LEIE monthly, and CMS has stated it expects providers to check at least that often to determine the exclusion status of current employees and contractors. Technically, providers need only screen vendors providing a service that is payable by a federal healthcare program. In practice, the best course of action is to screen all contractors, subcontractors, and employees of contractors using the same analysis used for hospital employees. This avoids issues caused by changes in vendor relationships that occur over time.
- **Checking for potential conflicts of interest.** Each organization should have strong policies in place concerning employee ownership of companies the hospital does business with and the acceptance of gifts and gratuities from vendors and physicians. The board of directors, the entire management team, all employed physicians and staffers in Purchasing, Internal Audit, and Compliance should complete

a conflict-of-interest disclosure form annually or semi-annually. They must be required to disclose ownership of vendors by grandparents, parents, children, siblings, and spouses, and the grandparents, parents, children, and siblings of the spouses.

- **Checking for physician-owned distributorships (PODs).** Because many vendors, particularly medical device manufacturers, often try to hide the fact that they have physician owners, vendors should be required to assert that they have no physician-owned distributors or investors. In March 2013, OIG stated that PODs are inherently suspect (essentially guilty until proven innocent) and that disclosure of ownership is insufficient assurance that no fraudulent activities are occurring.
- **Setting up ongoing vendor checks.** An important component of a comprehensive onboarding process is setting up systems to ensure vendors are checked periodically (ideally, it should be monthly) for any change in ownership, BA compliance, or security status.

Mitigation 4:
Respond effectively in an OCR audit
Hospitals could be audited by OCR or other government agencies focused on HIPAA compliance. If a hospital is audited for a data breach or even a complaint, it should carefully read the request and send all of the information requested—and only the information requested. Some organizations view desk audits as less of a burden than on-site audits. This is true in one sense (an overheard remark while an auditor is on site can lead to a new area of investigation), but documentation must stand completely on its own in a desk audit.

There will be no opportunity to clarify or provide additional information, so it's important to index all submitted information thoroughly and provide a cover letter describing each tab's content. Form is not as important as substance, of course, but it's wise to provide information in as organized a manner as possible.

1. Third Annual Benchmark Study on Patient Privacy & Data Security, Ponemon Institute, December 2012.
2. "Breaches Affecting 500 or More Individuals." U.S. Department of Health & Human Services. http://bit.ly/15nN3cQ

Now Available!

Research Compliance Professional's Handbook *Second Edition*

Get HCCA's practical guide to building and maintaining a clinical research compliance & ethics program

Clinical research is highly regulated, so the role of compliance professionals is vital to meeting the demands of a wide range of governing entities.

This new edition of the handbook offers comprehensive, up-to-date guidance to get you on the right track.

Written by experts with hands-on experience in clinical research compliance, this book is intended for anyone with compliance duties or a need to understand such key areas as:

- human subject protections
- biosecurity and biosafety
- research using animals
- scientific misconduct
- conflicts of interest
- privacy and security
- grant and trial accounting
- effort reporting
- clinical trial billing
- records management
- data and safety monitoring
- role of oversight entities
- auditing & monitoring
- integrating research compliance into corporate compliance

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Visit **www.hcca-info.org/books** *to order.*

by Paul P. Jesep, JD, MPS, MA

Surveys—Paper, electronic, or both?

» Paper surveys still have great value to an organization.
» Do not replace surveys with online tools. Leverage paper surveys as tools.
» A paper survey lends itself to sensitive information by providing more anonymity.
» Paper surveys give the compliance officer another opportunity to directly engage with staff.
» The effort taken to compile and analyze data from paper and online surveys is still a wise investment.

Paul P. Jesep *(PJesep@gmail.com) is an ethics and compliance consultant and is employed part-time as the Compliance Officer for Hometown Health Centers in Schenectady, NY.* *bit.ly/in-PaulJesep*

It may surprise some, but the format of a survey (i.e., paper or online) can have a direct impact on response rates and how forthright respondents are in sharing feedback. Of course, there are studies regarding which format is best. Surprise—they contradict.[1-5]


Jesep

Weighing the pros and cons

There are obvious benefits to going paperless. Gathering information online is fast, easy, and readily accessible. It saves paper, sparing you the disapproving looks from spirited, environmentally minded colleagues. Nor are there worries about safely storing and eventually shredding responses. Incidental benefits include saving money in ink, staples, filing cabinets, and wear and tear on the copier.

Online surveys make information easier to analyze, whether the focus, for example, is on a specific department or broken down by job title or years of service. Cross-referencing data becomes instantaneous.

Ultimately, most people work in fast-paced environments where time is of the essence. In the technology age, someone juggling multiple tasks in a busy office would likely prefer to zip through a short online survey rather than doing one by hand. In the paper world, results have to be tabulated manually, which is a drain on resources.

In weighing the option of paper or electronic surveys, consideration must include the sensitivity of the data or information to be gathered. If the board of directors is using an organization-wide survey to determine the perceived honesty of the chief executive officer (CEO) and chief financial officer (CFO) and the overall ethical environment, online might not be the way to go. Depending on the culture of an organization, some may perceive (regardless of misplaced fears and assurances of confidentiality) that they will leave an electronic footprint and their answers tracked back to them, with retaliation to follow.

Although the electronic survey has an important place in compliance, it comes (in addition to the limitation just cited) with other drawbacks that shouldn't be overlooked. An electronic survey depersonalizes part of the process. A paper survey is another opportunity for a compliance officer to engage with the team at meetings or during his/her walk-through of the building, which nurtures personal relationships.

Recently, a doctor-friend at a prestigious hospital told me he had never met anyone from his Compliance department, didn't know who any of the compliance staff were, and had never seen anything posted that struck him as compliance related. Yikes. This might be an extreme example to use, but the compliance officer should look for every opportunity to "get out there" and see and be seen. Handing out a paper survey and underscoring the importance of answering it and dropping it in a locked compliance box is another way to meet and greet.

Practically, paper also enables the respondent to go back to change an earlier answer after having gone through the entire survey. He/she can reflect on the whole process. Online surveys tend to be categorized or compartmentalized in a way that sometimes limits the ease in modifying an earlier response.

Electronic surveys require a level of skill to manipulate their design and dissemination. This could require delegating the task to a colleague or subordinate who may have access to who answered and how something is answered. Case in point is the rogue information technology (IT) manager who can go undetected in reading incoming and outgoing emails without authorization. It's not unheard of, and happens a lot more than the CEO, CFO, or chief operating officer (COO) may realize.

As referenced above, who and what you're surveying should play a role in the tool selected. Surveying staff about their satisfaction with salary, benefits, vending machines, comfort of the break room, and other relatively innocuous matters that play a role in organizational morale lends itself to an online survey.

In contrast, surveying staff with paper about possible theft, double billing in government contracts, or workplace bullying by supervisors and senior managers may provide greater comfort to respondents. These anonymous surveys, which can include typed responses for questions requiring a few sentences, can be left in a locked box that only the compliance officer can access, and he/she has a direct line to the board of directors.

Today, the mantra is "all things paperless." It's short-sighted. Paper should always have a place in an organization. It should be thought of as a valued tool for the right situation, not an outdated method of gathering information.

1. S. Z. Berg: "Paperless Life May Help You in Multiple Ways," February 9, 2015, *DailyFinance.com*. Available at http://bit.ly/1ESUd8uj
2. Susan E. Wyse: "Which is More Effective: Paper-Based Surveys or Online Surveys?" *Snapsurveys.com*; January 31, 2012. Available at http://bit.ly/1S1JxpW
3. Kelvin Stiles: "Paper Surveys vs Online Surveys – Which One's Better?" *Surveycrest.com*; March 14, 2013.. Available at http://bit.ly/1EXxu44
4. David M. Shannon, Todd E. Johnson, Shelby Searcy, and Alan Lott: "Using Electronic Surveys: Advice from Survey Professionals," *Practical Assessment, Research & Evaluation Journal;* 2002. Available at http://bit.ly/1ESUikB
5. A. M. Croteau, John Molson, M. Miquel, and L. Dyer: "Employee Reactions to Paper and Electronic Surveys: An Experimental Comparison." Professional Communication, *IEEE Transactions* (Vol. 53, Issue 3), September 2010. Available at http://bit.ly/1AaRAeI

by Janice Anderson and Ken Briggs

Creating effective solutions for data privacy concerns in clinically integrated networks

» Clinically integrated networks are becoming the cornerstone of the healthcare delivery system.
» Privacy laws pose complex and contradictory hurdles for successful integration.
» Data exchange through networks has significant liability and regulatory implications.
» Certain structures of clinically integrated networks are more effective than others.
» Networks should investigate different options to structure the network in light of applicable state and federal privacy laws to determine the most efficient solution.

Janice Anderson *(janderson@polsinelli.com) is a Shareholder in the Chicago office and* ***Ken Briggs*** *(kbriggs@polsinelli.com) is an Associate in the Phoenix office of Polsinelli PC.*

The healthcare system is transitioning from one that ties payment to the quantity of services rendered to one that ties payment to quality. One milestone of progress, described by the Secretary of Health and Human Services on January 26, 2015, is the goal that by 2018, half of all Medicare payments are projected to be tied to the quality of the services provided.[1] One way to achieve this goal is through payment models that require the use of clinically integrated networks or accountable care organizations (ACOs). These organizations establish new ways for providers to work together to enhance the quality of services across the healthcare spectrum. Data—derived from patient information—is the fuel for these new delivery systems. Patient information also provides the measure for how well the services are being provided, and as a result, is the basis for how providers are compensated in these new delivery systems.


Anderson


Briggs

Laws that impact how providers may use and disclose patient information in the context of these new delivery systems have not kept up with changes to how care is delivered. Specifically, healthcare is being provided increasingly through clinically integrated delivery systems, which require the sharing of patient information in ways that are different from the past. These networks of providers need to be carefully structured to efficiently navigate privacy laws, and each structure may be different depending on the network's purpose, the interests of the participants, and applicable state and federal privacy laws. This article will provide an outline of modern delivery systems, discuss the impact of state and federal data privacy laws, and highlight trends of how networks are being structured to address privacy requirements.

Successful networks and the exchange of information

Providers can work together in a number of ways. Integrated networks of providers are

usually composed of legally separate providers, many of which render different types of services. Networks include those built around achieving quality metrics (such as lowering readmissions) or enhancing the flow of information among local providers who treat the same patients. Accountable care organizations, physician hospital organizations, and independent practice associations are examples of structures that may become clinically integrated networks.

The basic structure of a network involves a "hub" or central entity, whether it is a separate administrative entity or a participant in the network, that enters into contracts with providers to secure participation in the network. Almost any type of provider can participate in a network, including most commonly individual physicians, physician groups, and hospitals. The central entity usually performs management and administrative services for the network, such as engaging vendors, contracting with payors, and analyzing data that flows through the network to assess and improve the quality and efficiency of care.

To achieve their purpose of improving quality or providing services more efficiently, networks must invest in infrastructure to share information, which may be achieved by creating a health information exchange, joining a separate exchange, or by sharing the same system. These information systems make the transfer of data between providers easier, both in terms of technological advantages and sharing the costs of infrastructure improvements among providers. Because of the infrastructure, time, and costs involved in developing the systems, decisions regarding information exchange should be a principle consideration when structuring the network.

Health information exchanges can be formed privately among participants, through a regional exchange, or through a national public exchange. Typically, these exchanges have separate technologies that connect to the electronic health records (EHR) systems used by individual participants. The patient information can be transmitted through the exchanges in different ways, as needed by the network. For example, an exchange may be set up to allow participants to send data to another participant directly (a directed exchange) or to request data from another participant (a query-based exchange).

Providers that are closely integrated are moving towards sharing the same system of health records. This "shared medical record" arrangement means that one system maintains the entire record of the patient; there is no exchange of information.

Providers that are closely integrated are moving towards sharing the same system of health records. This "shared medical record" arrangement means that one system maintains the entire record of the patient; there is no exchange of information. These shared systems promote the most integrated arrangement, and as a result, require the most operational adjustments to use one system.

Efficient exchange of information is essential for clinically integrated networks to use the data to shape practices and outcomes of the network. Once the technology and ideal method of sharing information is established, the privacy laws must be analyzed to determine appropriate safeguards.

The obstacle of data privacy laws

State and federal laws impose different and sometimes conflicting obligations on how data may be used in modern healthcare arrangements. Legal obligations may affect how the network participants document their arrangement, communicate with patients, and use or disclose information among participants.

Most, if not all, states have enacted laws that impact the flow of information among providers, and most state laws apply even to information exchange in integrated arrangements. States impose requirements, conditions, or limitations on how information is shared through statute or regulation. Medical information is regulated by states in a combination of ways:

- States may have a defined series of statutes that regulate all medical information.
- The use or disclosure of medical information may be restricted through licensing requirements according to the type of provider. For example, states may impose additional or different patient privacy requirements on a hospital, but not a physician.
- States may impose requirements on specific types of medical information (e.g., communicable diseases, mental illness, substance abuse).
- States may impose specific data privacy obligations on specific arrangements, such as health information organizations.

The entire body of a state's regulation of medical information should be scrutinized to identify how each of the participants and the network can maintain compliance with these regulations in a new delivery system.

The federal government imposes restrictions on the use or disclosure of patient information primarily through the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The regulations of the HIPAA Privacy and Security Rules are set forth in 45 C.F.R. Parts 160 and 164. HIPAA regulates the use and disclosure of patient information through the Privacy Rule and imposes safeguards and protections on electronic patient information through the Security Rule.

HIPAA applies to covered entities and business associates. Covered entities include health plans and healthcare providers; business associates are entities that perform services for or on behalf of covered entities. HIPAA affects integrated provider networks in two important ways. First, the law requires entities subject to HIPAA to implement technical, physical, and administrative safeguards to protect the storage and transmission of patient information. These safeguards must take into account the provider's participation in the network and the services provided between them. Second, HIPAA imposes restrictions on how providers may use and disclose information throughout the network, depending on how the network is structured.

In addition to HIPAA obligations, federal law also restricts the ability of substance abuse treatment providers to share information, even in the context of integrated care. The substance abuse privacy regulations (at 42 C.F.R. Part 2) extend to other participants in a network when substance abuse information is shared. These regulations, enforced by criminal penalties, require even higher standards, safeguards, and protections applicable to substance abuse records. Industry stakeholders have called into question the efficacy of the regulations and the government has been considering modifications. Regardless of how these regulations are revised, all of the participants in a network should be aware that sharing substance abuse information protected by Part 2 is restricted by federal law.

Networks and their participants must comply with HIPAA where it conflicts with state law, unless the state law provides a greater right of privacy or a greater right of access to

the patient. The privacy laws adopted by states may not be consistent with HIPAA, which sometimes results in a patchwork of obligations that relate to the same conduct. Access, opt-out, and consent protections are categories of state regulations that are most often more stringent than HIPAA. States may also, however, enact requirements necessitating specific communications to patients, obligating the network to maintain information in a certain way, or requiring the network to develop and follow specific policies. Where these state laws offer greater privacy or access rights than HIPAA, networks must operationalize these obligations through network policies and sometimes in individual participant policies. These obligations also must be observed in the network's technology. For example, the data sharing systems must permit certain information to be sequestered or blocked before it gets to the network. The technologies should also be able to indicate when consents are required or obtained, and trigger and document communications provided to the patient.

In addition to how participants may use and disclose information, most states and HIPAA have adopted regulations describing minimum standards for safeguarding patient information or for performing certain notification obligations in the event of a breach of patient information. These breaches often trigger obligations to notify the patient, state and federal governments, the media, and even consumer protection agencies—all within specific deadlines. Network participants must consider the exposure to liability resulting from non-compliance with laws or uses or disclosures not permitted by the laws. These liabilities—and the obligations triggered by the liabilities—should be considered when the network is organized.

Participants should understand how these obligations apply to the other participants in addition to their own obligations, because entering into a contractual relationship with other entities could expose the participant to new obligations. Given that networks are cutting-edge arrangements, breaches of information pertaining to a network can be very complex to investigate and resolve. Although some breaches may be relatively straightforward, such as a lost portable device, other breaches involving a network may be more complex and involve more than one participant.

Participants should understand how these obligations apply to the other participants in addition to their own obligations…

Trends in efficiently navigating patient privacy laws

Networks that have succeeded in bringing participants together in a way to achieve effective integration share the motivation to deal with data privacy laws from the beginning. Networks should consider how to address patient rights that may be protected by law and relate to providing patients a chance to opt out of data sharing through an exchange or a right to consent to the use of an exchange for sharing certain information throughout the network. These laws need to be identified at the outset of the arrangement to ensure that the participants are aware of their responsibilities to discuss the rights with the patient and to secure any required authorizations. The ability of the exchange software to sequester, block, flag, or remove information from the network should be specifically verified with the vendor to ensure that the software can accommodate patient rights or requests. If a patient with a

right to opt out does not wish to be included, or if certain information is subject to consent requirements prior to release, the software should be able to accommodate these issues without fail.

In addition to the patient rights, the way in which network participants document their relationship and hold themselves out to the public as participating in a network will affect how privacy regulations apply to the network. A network may be able to achieve greater flexibility for the exchange of patient information, however, by organizing itself as an organized healthcare arrangement (OHCA) under HIPAA.[2] Structuring the network as an OHCA permits network participants to exchange information more easily and may provide additional protection in the event of a breach of information. To properly organize the network as an OHCA, the participants must hold themselves out to the public as participating in a joint arrangement and participate in utilization review, quality assessment, and improvement activities, or payment activities where the financial risk is shared among the participants.

An OHCA can include only covered entities. Therefore, the network, along with other entities performing services for the network, would still need to enter into business associate agreements with the OHCA.[3] Participants involved in an OHCA should describe their participation in the OHCA and the permissible exchanges of information through the OHCA in each participant's Notice of Privacy Practices.

Agreeing to the security standards and privacy practices of participants in a network is essential, given the enforcement environment. The obligations of the parties as to how they may use and disclose patient information, and the minimum safeguards maintained by each of the participants, must be dictated through contract. The poor practices of one participant can lead to an impermissible use or disclosure of patient information across multiple, if not all, participants. "[I]f the Secretary determines that more than one covered entity or business associate was responsible for a violation, the Secretary will impose a civil money penalty against each such covered entity or business associate."[4]

The security of the network is only as strong as its weakest link. A serious breach of patient information can damage any provider relationship and, with the size of modern breaches, can cripple a network. Given the significant risk, the parties should dedicate serious effort to agreeing on the minimum security standards required of participants, and the expectations for the parties to discover, investigate, and report breaches of patient information. These expectations should be detailed in network documents and should be consistent with any ancillary agreements, including participation in a health information exchange and business associate agreements. In discussing these obligations, the participants should consider how to determine reimbursement for costs involved in the breach (including third-party consultants and costs to notify the patients) and how to allocate damages resulting from a breach.

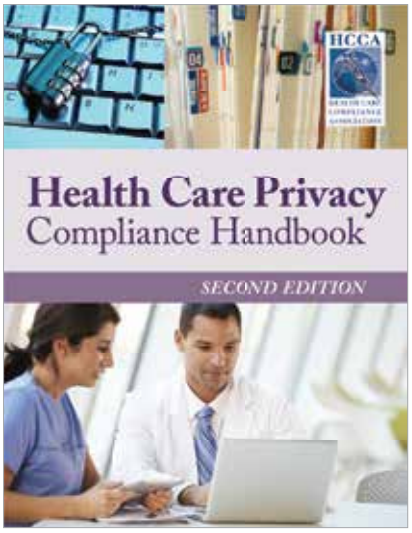
Conclusion

Successful networks have achieved that success by establishing the purpose and the trajectory of the network into the future, identifying the legal obligations of the network and each participant, and delineating the obligations and expectations in the network documents. Once this investment is completed, the networks can determine ways to navigate successfully through the obstacles of the data privacy laws and focus on delivering quality care.

1. Sylvia M. Burwell: "Setting Value-Based Payment Goals — HHS Efforts to Improve U.S. Health Care." *The New England Journal of Medicine,* January 26, 2015. Available at http://bit.ly/1Ehm5dQ (paywall)
2. 45 C.F.R. § 160.103.
3. 45 C.F.R. § 164.502(e).
4. *See* 45 C.F.R. § 160.402.

Health Care Privacy Compliance Handbook

NEW! Second edition available



SECOND EDITION

This second edition will help privacy professionals sort through the complex regulatory framework facing healthcare organizations. Written by the faculty of HCCA's Healthcare Privacy Basic Compliance Academy®, it offers up-to-date guidance on:

- HIPAA Privacy and Security
- HITECH and the Omnibus Rule
- FERPA
- The Federal Privacy Act
- 42 CFR, Part 2
- Privacy and Research
- Vendor Relations
- Payor Privacy Issues
- Auditing & Monitoring

Health Care Privacy Compliance Handbook, Second Edition
(Prices are as listed and considered net of any local withholding taxes applicable in your country of residence.)

QTY		COST
_____	HCCA members: $149	$ _____
_____	Non-members: $169	$ _____
_____	Join HCCA: $200	$ _____

Non-members, add $200 to join HCCA, and pay member prices for your order. (REGULAR DUES $295/YEAR)

TOTAL $ _____

Please type or print your mailing information below:

○ Mr ○ Mrs ○ Ms ○ Dr

HCCA Member ID

First Name MI

Last Name

Job Title

Name of Employer

Street Address **(NO PO BOXES)**

City State Zip

Phone

Email

Make check payable to HCCA and mail to:
HCCA, 6500 Barrie Road, Suite 250
Minneapolis, MN 55435

Or fax your order to: 952-988-0146

○ Check enclosed (payable to HCCA)
○ Invoice me
○ I authorize HCCA to charge my credit card *(choose card below)*

Due to PCI Compliance, please **do not provide any credit card information via email**. You may email this form (without credit card information) and call HCCA at 888-580-8373 or 952-988-0141 with your credit card information.

CREDIT CARD: ○ American Express ○ MasterCard ○ Visa ○ Discover

Credit Card Account Number

Credit Card Expiration Date

Cardholder's Name

Cardholder's Signature

Prices are subject to change without notice. Shipping is complimentary to addresses within the continental United States via FedEx Ground. Please include your full physical address. Products shipped via FedEx cannot be delivered to a PO box. Addresses outside the continental United States are subject to standard shipping rates: Contact HCCA for pricing. Please note that HCCA will charge your credit card the correct amount should your total be miscalculated.

by Jon H. Klein, JD, CHC

The lure of Part D reimbursement: Should dentists fish or cut bait?

» Review provider contracts in response to legislative changes.
» Dialogue with non-compliance staffers to assess impacts of new legislation.
» Monitoring efforts include matching NPI code numbers to the treating physician.
» Know risks associated with patient surcharges and co-pays.
» Cross-train in dental/medical for compliance staff involved in integrated care.

Jon H. Klein *(kleinj@interdent.com) is a Compliance Officer for Capitol Dental Care, an Interdent company located in Salem, OR.* bit.ly/in-JonKlein

Under a recent rule change, the Centers for Medicare & Medicaid Services (CMS) will compel dentists to enroll in Medicare to order medications for patients covered by its drug program, known as Part D. Dentists (and other clinicians who fall within the CMS definition of "physician"[1]) must enroll or opt out via affidavit to the regional Medicare carrier by June 1, 2015—or face the risk that a pharmacy with a Part D eligible patient will not be reimbursed by Medicare for the dentist's prescription. However, CMS will delay enforcement of this interim Final Rule until January 1, 2016. In effect, CMS will continue to reimburse the pharmacist for a Part D-covered prescription until the end of the year, even if the dentist fails to meet the June 1 enrollment deadline.


Klein

Enroll, opt out, or do nothing

Until recently, Medicare had not been on the radar for most dentists, because the program covered few dental procedures. Plans differ, but most cover exam, x-rays, cleaning, prophylaxis, and fluoride, with a $500 benefit limit per policy year. However, with a change in the healthcare landscape, many dentists have begun to participate in Accountable Care Organization/Coordinated Care Organization (ACO/CCO) arrangements or serve as downstream providers for Medicare Advantage carriers that offer a limited set of dental services (e.g, reconstruction of the jaw following accidental injury, extractions done in preparation for radiation treatment for neoplastic diseases involving the jaw, and examinations as part of a work-up prior to renal transplant surgery or heart valve replacement[2]) to their Medicare patients. Primarily, it is these clinicians and their non-dental counterparts who must decide to enroll or opt out, and many are concerned that such enrollment could trigger other requirements under the Medicare umbrella that do not support dentistry (i.e., a requirement that the patient complete a Medicare Advance Beneficiary Notice for a procedure as simple as filling a tooth).

Maintaining the status quo and taking no action is not an option for the physician/dentist who treats or intends to treat the

Medicare-eligible patient. Clinicians who do not treat Medicare patients are not required to do anything. However, those dental providers on the lookout for new markets and new revenue streams should take note that the number one out-of-pocket healthcare expense for baby boomers is dental healthcare.[3]

At a minimum, the dentist with a book of Medicare patients who refuses to enroll or opt out can expect to get an ear full from the uncompensated pharmacist who shares with the patient that "Your dentist is not complying with federal law." The pharmacist does not get reimbursed under Part D, because the prescription for that "tooth extraction" is classified as a medical benefit and that benefit is tied to a physician's enrollment.

Although the American Dental Association (ADA) disagreed strongly with the new interim Final Rule—and pushback on enforcement to January 1, 2016 from the initial June 1st date may have something to do with ADA lobby efforts—CMS held firm in its view that some action by dentists was required to save taxpayer dollars (i.e., closing the loophole that allowed some practitioners to prescribe drugs). So, while the dentist new to Medicare may balk at signing in to the government's PECOS database (that is, the Provider Enrollment, Chain and Ownership System), the intent of the law is to reduce overutilization—a concern that falls squarely on the shoulders of the compliance professional. The appropriate application for the dentist who chooses to enroll in the PECOS system is CMS 8550 - Ordering and Referring application, because it is the pharmacist who actually submits the bill for Part D reimbursement.

The decision to opt out of Medicare will—as counterintuitive as it seems—still allow Medicare Part D-eligible patients to receive prescription drug coverage. It is in taking no action that the patient risks loss of reimbursement for the drug benefit. Dental referrals to specialists (e.g., endodontists) are not covered by the new rule. The specialist can submit a Medicare claim without having to list the referring dentist. However, dentists ordering clinical labs or imaging services must enroll or opt out for providers of those services (e.g., oral pathologists) to be reimbursed by Medicare.

Those physician/dentists that serve Medicare patients and choose to opt out, must enter into a private contract with each Medicare patient. The contract requires that the patient acknowledge that the physician is no longer enrolled in Medicare and that the patient is obligated to pay for dental services. That private contract is yet one more document the compliance professional must add to the "documents to be retained" file.

Those physician/dentists that serve Medicare patients and choose to opt out, must enter into a private contract with each Medicare patient.

A beneficiary eligible for Medicare drug reimbursement who sees a non-enrolled dental provider would have to file his/her own claim for reimbursement with federal form DD 2642 – Patient's Request for Medical Payment, or pay the full amount of the prescription. Patients who lack dental coverage may still benefit from Medicare Plan D by paying cash for dental services, then seeking reimbursement for the drug coverage benefit under Medicare Part D. However, in that case Medicare would not reimburse the pharmacist if the dentist of the cash patient with Part D drug benefit had failed to enroll or opt out.

Once a dentist formally opts out, he/she is precluded from receiving Medicare reimbursement for a period of two years. This provision was expanded on April 15, 2015, when Congress passed the Medicaid Access and CHIP Reauthorization Act of 2015, which allows dentists and physicians to permanently opt out, as opposed to the two-year opt out period. Dentists interested in a permanent opt-out option may wish to wait until the June 16, 2015 effective date of the Act. The choice to opt out is not without consequences, because it can limit a clinician's short- or long-term career options. And, the compliance professional must also monitor to confirm that the newly opted-out physician/dentist doesn't happen to do a favor for a colleague and treat a Medicare patient "just this one time" and bill Medicare under his/her colleague's National Provider Identifier (NPI) code. This constitutes fraud under Medicare regulations and is a violation of the False Claims Act.

As the January 1, 2016 enforcement deadline approaches, it would be prudent for the compliance professional, who works for an organization that participates in a health-care arrangement, to review (or recommend legal counsel review) contracts, especially in circumstances where patients are Medicaid-eligible, such as within a state health plan. These contracts may include language that requires down-stream providers (such as dental care organizations) to look solely to Medicaid for payment and prohibit the provider from seeking payment in any form for covered services from Medicaid members. The contract may not permit a provider to be charged a surcharge for prescription drugs.

It is possible that if a Medicare Advantage Plan member is required to go out-of-pocket and pay for a drug that would typically be covered under Medicare Part D (as a result of the physician/dentist's failure to "opt in or opt out"), that payment could constitute a surcharge. By default, this may force additional compensation onto the patient and, therefore, violate a contract provision prohibiting a surcharge. Prescription drug coverage does fall into the "medical services basket" and, therefore, is outside dental covered services. However, the last thing a compliance professional (and an organization as a whole) needs is a creative lawyer looking for a case where there isn't one.

…the last thing a compliance professional (and an organization as a whole) needs is a creative lawyer looking for a case where there isn't one.

Conclusion

The coordinated-care market and Medicare Advantage markets are highly competitive. Providers and carriers want to ensure that their dental providers are responsive to their members' needs. This may require that organizations have their dental providers enroll in Medicare Part D, even if the dentist's contact with Medicare patients is minimal. Not only would this provide an additional revenue stream for the organization, but it might just keep the member base happy, to say nothing of those who want to be paid when they dispense prescriptions for tooth pain.

1. For "physician" definition, see 42 CFR 405.400.
2. CMS: Medical Dental coverage. Available at http://bit.ly/1F4Uf34
3. Tom Wall, Kamyar Nasseh, and Marko Vujicic: "Per Patient Dental Expenditure Rising, driven by baby boomers." *Health Policy Institute*, American Dental Association. Available at http://bit.ly/1IMrnEj

by Adam K. Weinstein, MBA, MPA, FACHE; Cindy Hart, LPN, CPA, CPC, CHC; and Walter E. Johnson, MSA, CHC, CRCMP, CCEP-I

Compliance 101

The seven essential elements, Part 5: Reporting & investigation

» Diverse personality types, comfort levels, and belief systems may determine how an employee prefers to report a problem or concern.

» Offering several reporting channels may increase the number of problems or concerns reported.

» Onsite visits and regular communication may improve comfort levels of employees, thereby increasing the number of problems or concerns reported.

» Investigating reported problems or concerns reinforces the compliance message that reporting is encouraged.

» Employees participating in investigations may become more cognizant of the compliance program and decide to identify their preferred reporting channel.

Adam K. Weinstein *(aweinstein@nyp.org) is Vice President, Regulatory Affairs and Corporate Compliance at New York Hospital Queens in Flushing, NY.*
Cindy Hart *(cindy.hart@ctca-hope.com) is Senior Physician Compliance Specialist with Cancer Treatment Centers of America in Schaumburg, IL.*
Walter E. Johnson *(walter@wejohnson.org) is a Compliance Consultant residing in North Potomac, MD.* */in/walter16* *@walter_johnson1*

Part 4 of this series was published in the May 2015 issue of Compliance Today.

Impressive, the compliance program is evolving. The board of directors, senior leaders, compliance officer (CO), and compliance team are engaged. Routine education, auditing, and monitoring programs are established, documented, and have routine schedules. Awareness is increasing and the corporate culture is gradually incorporating compliance into operations.

Although the program seems established, the hotline is not demonstrating significant activity. From another perspective, the CO and compliance staff are receiving direct calls from internal and external business partners. Is there a problem if one reporting channel experiences higher volume than another channel? Fluctuating activity levels between reporting channels does not necessarily represent a problem. Analyzing activity levels may provide information to gain an understanding of the corporate culture. This information helps to identify methods that require attention and/or adjustments.


Weinstein


Hart


Johnson

Reporting

Employees may use a variety of methods to report potential problems or raise concerns.[1]

It is important for organizations to offer and promote as many methods as possible. Employees are diverse. They have different personality types, traits, comfort levels, and belief systems driving their behavior. Offering different reporting methods allows employees to report problems and concerns using the channel that feels most comfortable to them.

One segment of reporting includes accommodating employees in order to obtain information that may protect the organization. Another segment of reporting includes protecting employees by fostering a culture that ensures there will be no retaliation for reporting a problem or concern.[2] Employees want to feel stable and secure. Additionally, they want to feel confident in their decision to report. This is where the non-retaliation policy is most effective. A trait that plays a role with some employees is insecurity and lack of confidence. Insecure or non-confident employees may want to avoid the feeling that their report could demonstrate a lack of industry knowledge, a misunderstanding of the organization, or even misunderstanding the reported problem. Additionally, an employee may want to avoid causing an unnecessary problem.

Employees differ. According to Myers-Briggs, psychological differences consist of four opposite pairs, or dichotomies, resulting in 16 possible psychological types. The four dichotomies are extraversion/introversion, sensing/intuition, thinking/feeling, and judging/perceiving.[3] For example, an extravert enjoys frequent interaction and receives energy by being with people. An extrovert employee may prefer an in-person visit to the CO's office to talk through a problem or concern.[4] From another perspective, an introvert employee may prefer an anonymous call to the hotline or prefer placing an anonymous tip in a suggestion box. Opposing arguments surround the Myers-Briggs approach and of the frequently used exam.[5] The intention of the authors of this article is not to provide an analysis of each dichotomy and psychological type; rather we recommend consideration of personality types when determining reporting methods for your organization.

Although available resources may influence the structure and available reporting channels, consideration of psychological types is vital. COs or organizations must avoid developing one reporting channel or steering employees to the channel that leadership believes is the best one. In doing so, employees may feel neglected and reporting may be delayed or not occur at all.

In a recent Society of Corporate Compliance and Ethics article,[6] Joseph Murphy shares his experience of an investigation where an employee had pertinent information to assist with resolving an investigation. Murphy and his colleague had discussions with other employees prior to identifying this employee. When Murphy finally met with the employee, his response was, "I was waiting for you to call." This a perfect example of the need for establishing multiple reporting channels.

COs are not solely responsible for creating a culture that encourages employees to report issues and concerns; however, an empowering culture should be a priority of the CO. Murphy states, COs must have a presence outside of their office. When reporting a concern, employees must believe there will be a review and no retaliation. There are multiple approaches to establishing and maintaining employee confidence in the process. One approach is the "open door" policy and another is conducting site visits.

Does it matter whether the CO, compliance staff, compliance hotline, or suggestion box are receiving equivalent activity? The authors believe it is more important to have multiple reporting channels with fluctuating volume than limited channels with steady volumes.

A CO who receives more calls than the hotline may indicate that employees believe contacting the CO directly results in action. If the compliance staff receives more calls than the CO, it may indicate that employees trust the staff to report the problem confidentially to the CO and, if applicable, to follow-up with results. If a hotline receives more calls than the CO and compliance staff, it may indicate

employees prefer the anonymity of the hotline. Regardless of the reporting method, all problems require the due diligence of an investigation to prevent potential harm.

Methods of reporting

As mentioned above, people respond according to their personality and will select the most comfortable reporting method. Although companies should offer several reporting mechanisms, budgetary constraints may limit the offerings. A hotline that is managed by an external company can be expensive, depending on the volume of calls and the amount of detail desired in reports. An external company that manages a hotline can be contracted to simply accept calls, classify the calls into priority levels, and provide a written monthly report. Alternatively, an external hotline management company may prepare dashboards, real-time reporting for highest priority claims, and contact authorities in the event of a claim of physical abuse. A detailed contract is recommended for cost control.

The company should create a policy that describes the hierarchy of reporting methods, beginning with a report to the employee's direct supervisor, and moving up the chain of command. Suggestion boxes are common, but many misconceptions surround their use: (1) Is someone watching the suggestion box? (2) Are cameras focused on the area? (3) Will handwriting be recognized? (4) Does anyone actually read the suggestions? Electronic suggestion boxes can be perceived as suspicious. Can the claim be traced back to the claimant? Although it is recommended that employees initially report through their chain of command, no method should be discouraged.

Typically, external hotline companies send the hotline report to the CO. Others who may receive the report are Human Resources (HR) or the Legal department. The CO should implement alternate methods to handle situations where the offending party is the supervisor, HR staff, or even a member of the Compliance department. Anonymous hotlines are usually the best method for reporting these situations. Hotlines provide the best method for anonymous reporting and are perceived as the least likely method to result in retaliation.

The CO should monitor the effectiveness of each type of reporting method. Calculate volumes by month, quarter, or year, and compare them to prior periods. Analyze classifications of claims. Are most claims essentially HR issues (employee unhappy with some action taken by his/her supervisor), or are most claims targeting suspicious billing methods? Finally, the CO should monitor the investigation process and outcomes. Are most claims unsubstantiated? If most are unsubstantiated, what is the underlying cause that prompts the claims? The CO should educate employees on proper use of the hotline. Employees who understand the reporting policy, are engaged and empowered to utilize the hotline appropriately, and believe their company is ethical will help drive the corporate culture towards doing the right thing all the time.

Investigations

When conducting investigations, review documentation such as procedures, forms, spreadsheets, and other executed activities. The investigation should include engagement of the individuals who will help provide relevant information. When engaging these individuals, the discussions should occur in person or by telephone. The investigator should begin by reassuring the person that no prejudgments have been made; the investigator is seeking the truth, and misconduct will be handled according to company policy. The person responding to the investigator should be confident that all responses will be confidential to the fullest extent possible.

A new CO may be required to report on current investigations. Where should the CO

begin? One clear way to start is to inquire about the nature of current investigations and review investigation activity notes. Request copies of past investigations and refer to them to set the groundwork for your investigation notes. As you complete this process, you will be able to ascertain whether or not your resolution is sufficient to adhere to regulatory guidelines.

It is imperative to maintain pristine records of investigations. It is also important to provide feedback to all complainants. Often, assuring the complainant that an investigation is underway and providing an expected timeline for completion will appease the complainant.

As the CO, you should become familiar with "hot targets." The CO should begin by becoming familiar with past investigative reports issued by accrediting agencies on the local, state, and federal level. In addition, review the Annual Work Plan published by the Department of Health and Human Services (HHS) Office of the Inspector General (OIG). The OIG also issues fraud alerts. Active participation on Health Care Compliance Association (HCCA) online discussion boards is an excellent way to discover hot targets.

Next, consider reviewing compliance with regulations for a particular process or department within your organization, such as security management, workforce security, or the Pharmacy department.

Security management

Complete a risk assessment of potential risks and vulnerabilities related to confidentiality, integrity, and availability of electronic protected health information (ePHI). Although the Health Information Portability and Accountability Act (HIPAA) Security Rule does not require entities to purchase particular technology, your organization may find that new hardware, software, or services are necessary to adequately protect health information.

Workforce security

Implement policies and procedures to ensure all members of your organization's workforce have appropriate access to ePHI. Appropriate access includes limitations for workforce members who should not access ePHI. Visit the websites of the OIG and the Office for Civil Rights (OCR) for information on appropriate access (*http://1.usa.gov/1cnZW7f*).

Pharmacy department

Review previous audits and verify the effectiveness of the actions implemented. Design an audit to identify the presence of common pharmacy errors, such as: (1) name tags that clearly identify a pharmacy technician vs. a pharmacist, (2) supervision of technicians by the pharmacist and proper labeling of medications on shelves, including the number of pills remaining in the bottle, (3) accuracy of records for controlled substances, (4) Schedule II inventory and dispensing records separate from Schedule III-V records, and (5) evidence of biennial inventory. These and other common pharmacy errors can be found online at *http://bit.ly/1dfASk7*.

Conclusion

You have come a long way from your first day as CO and can feel confident that your organization is progressing towards the fulfillment of an effective compliance program. The key is impeccable recordkeeping, consistent follow-up, and your team of professionals working together to establish a process where investigation findings are real, necessary, and making a difference for your organization.

1. Debbie Troklus and Greg Warner: *Compliance 101*. Third Edition. September 1, 2011. Health Care Compliance Association.
2. Department of Health and Human Services, Office of Inspector General: OIG Supplemental Compliance Program Guidance for Hospitals. January 31, 2005. Available at http://1.usa.gov/1i2FSmB
3. The Myers-Briggs Foundation: MBTI Basics. Available at www.myersbriggs.org
4. Dan Buettner: "Are Extroverts Happier Than Introverts? Insight into differences between two personality types." *Psychology Today*. May 14, 2012. Available at http://bit.ly/1HnBgrdh
5. Joseph Stromberg: "Why The Myers-Briggs Test Is Totally Meaningless." *Vox*. July 15, 2014. Available at http://bit.ly/11HDDre
6. Joe Murphy: "I've been waiting for you to call." The Last Word, *Compliance & Ethics Professional*. December 2014, page 90.

Congratulations, newly certified designees!

Achieving certification required a diligent effort by these individuals. Certified individuals promote organizational integrity through the development and operation of effective healthcare compliance programs.

Certified in Healthcare Compliance (CHC)®

- Dawn Backlund
- Carl Baranowski
- Sue Bayer
- Dawn Bloomer
- Katherine B. Bornstein
- Lauren N. Brown
- Christine I. Censon
- Angela Chadwick
- Kay Kay Chan
- Leigh B. Collier
- Leslie M. Conner
- Amanda V. Cross
- Angelique M. Culver
- Kelly Degler
- Beth DeLair
- Daniel N. Dube
- Joseph P. Dutson
- David Empey
- Molly S. Fleming
- Mark J. Fox
- Sara French
- Jane M. Fyffe
- David E. Garrison
- Enami Y. Gilbert
- Adam Gordon
- Shelby Gorman
- Margaret Griffiths
- Dawn Hansen
- Mia R. Harmon
- RoxAnne Y. Harris
- Kelly Henneman
- Michele Hennessey
- Shannon R. Hochstein
- Gloria Hoertner
- Kimberly G. Huey
- Jayne Hughes
- Brandon M. Ingram
- Colette D. Jackson
- Jesica M. Jensen
- Tina Kassis
- Dawn Michelle Kinneer
- Alton F. Knight
- Joshua R. Larson
- Sonya F. Lawrence
- Linda A. Le
- Megan A. Leon
- George A. Lewellyn
- Kathy A. Lindgren
- Karen M. Linz
- Jeffrey S. Loesch
- Caroline S. Louey
- Brenda K. Manning
- Charlotte A. Marz
- Richard A. Meeks
- Jonathan Melendez
- Pamela Meliso
- Albert Meyer
- Tiffany J. Miller-Kennedy
- Phyllis T. Molyneux
- Kathryn Mortensen
- Patrick S. Mullally
- Jimmy B. Perren
- Christine Peterson
- Channon C. Pifer
- Benjamin B. Presley
- Amber D. Quinton
- Mike S. Reisinger
- Nisha Roberts
- James Rose
- Katie Rudi
- Ahmed Salim
- Teresa Schorr
- Suzanne Sheldon-Krieger
- Karen Shell
- Andrew Shine
- Jesse A. Shipley
- Amy K. Sholis
- Elizabeth Strammiello
- Bart M. Sturdy
- Brittani Summers
- Noelle Valentine
- Francine D. Wachtmann
- Andy Wampler
- Sharon Westlake
- Brent T. Wilson
- John D. Wyckoff

Certified in Healthcare Research Compliance (CHRC)®

- David Behinfar
- Jennifer S. Dawson-Tibbits
- Dawn Pedinelli

Certified in Healthcare Privacy Compliance (CHPC®)

- Debby J. Andruss
- Heidi L. Baker
- Karlene M. Begay
- Denise F. Berger
- Kevin P. Cahill
- Susan L. Dahl
- Veronica Dale
- Cheryl Field
- Rebecca Ford
- Kim Gilbert
- Heather Hughes
- Monica Lareau
- Julie K. Maroo
- Janella L. McCants
- Monica McCarthy
- Daniel McManus
- Maria Mojica
- Melinda Montoya
- Douglas J. Nelson
- Jim Parks
- Elizabeth N. Pitman
- Ed Pruis
- Deborah A. Reif
- Mark R. Schneider
- Lauren A. Schultz
- Laurel A. Sweeney

CCB offers these certifications: Certified in Healthcare Compliance (CHC)®, Certified in Healthcare Compliance Fellow (CHC-F)™, Certified in Healthcare Research Compliance (CHRC)®, and Certified in Healthcare Privacy Compliance (CHPC®). To learn more, please contact us at ccb@compliancecertification.org, visit *www.compliancecertification.org*, or call 888-580-8373.

Want to become

Certified in Healthcare Compliance (CHC)®?

BE RECOGNIZED for your experience and knowledge!

The Certified in Healthcare Compliance (CHC)® designation demonstrates expertise in the healthcare compliance field. Earn yours today:

- Meet eligibility requirements in both work experience and continuing education
- Pass the CHC exam
- Maintain your designation by earning approved continuing education units

For more details on earning and maintaining this designation, please find the *CHC Candidate Handbook* or other information at **www.compliancecertification.org** under the "CHC" tab.

More questions? Email **ccb@compliancecertification.org**.

Hear from your peers

Valerie Puckett, CHC
Vice President,
Chief Ethics and Compliance Officer
McKesson Health Solutions
Alpharetta, GA

Why did you decide to get certified?

I decided to seek the CHC certification many years ago, when the profession was brand new. I reviewed information about the various compliance organizations, and found that the HCCA was the organization that had the best information for healthcare compliance initiates, and wanted to learn more. Thus, I attended an Academy and passed my certification test.

How do you feel the CHC certification has helped you?

This certification confirms that you know the field, have interest in learning more, and that you stay up to date by completing our mandated continuing education.

Would you recommend that your peers get certified?

Yes! If you want to stay in this industry and show that you have what it takes, get the certification germane to your business.

CHC™
Certified in Healthcare Compliance

HCCA *welcomes* NEW MEMBERS

ALABAMA
- Ashley Dean, Birmingham Gastroenterology Associates
- Tracy Linville, Widener University

ALASKA
- Wendy Rice, Kenaitze Indian Tribe

ARIZONA
- Diana Alvarez, Tenet/Phoenix Health Plan
- Michelle Vega-Lorenzo, Southwest Behavioral Health Services

CALIFORNIA
- Brenda Adams, Mercy & Memorial Hospitals Bakersfield
- Zenaida Aguilera, La Clinica
- Steve Baghoomian
- Mark Bradshaw, Alecto Healthcare Services
- Yevgenia Brown, Molina Healthcare Inc
- Cynthia Caldwell, Protransport-1
- Allison Cova, Dignity Health
- Lavetta Cross, HICCA
- Purvi Dave, The Ensign Group, Inc
- Pamela Delbridge, Pathnostics
- Cindy Goodman, L.A. Care Health Plan
- Ellen Hardin
- Melissa Hernandez, Accumen Inc
- Shannon Hochstein, Kern Medical Center
- Vikki Jenkins, Dignity Health
- Ellie Kamkar, Sutter Health Palo Alto Medical Foundation
- Debbie Lew, Ernst & Young, LLP
- Sharon Lewis, Primeau Consulting Group
- Solange Marvin, CalOPTIMA
- Han Nguyen
- Emy Robles, St. Joseph's Medical Center
- Gurinder Sarai, College Medical Center
- Narinder Sohal, Kern Medical Center
- James Tatum, Alliance HealthCare Services
- Daniel Teget, Jewett and Associates, Inc
- Mayra Villalta, Cedars-Sinai Health System
- Rita Wasley, Dignity Health

COLORADO
- Melissa Ellis, Envision Healthcare
- Danielle Langley, Touchstone Health Partners
- Mary Schumer, University of Colorado Hosptial
- David Scott, Peak Vista Community Health Centers

CONNECTICUT
- Linda Lutz, Saint Francis Hospital and Medical Center
- Pamela Meliso, The Corridor Group

DELAWARE
- Pamela Benton, Nanticoke Health Services
- Angela Nobles
- Edward Okonowicz, Christiana Care Health System
- Laura Weeks, Bayhealth Medical Center

FLORIDA
- Thomas Anderson, Diversified Service Options, Inc
- Carlos Arias, Access Health Care
- Cynthia Baron
- Rosa Bowling, Physician Partners of America
- Steven Chew, Tampa General Hospital
- Linda Chidlow, Chapters Health System
- Alisa Duke
- Wes Fischer, The Health Insurance Store
- Kym Grabman, Celebration Obstetrics & Gynecology
- Leslye Hagarty, Celebration Obstetrics & Gynocology
- Vinnette Hall, Broward Health
- Elizabeth Hodge, Akerman LLP
- Margaret Jagger, LIBERTY Dental Plan
- Noni Jefferson, Broward Health
- Janet Jones, Parallon Business Solutions
- Lee Lasris, Florida Health Law Center
- Brian Martens, HHS-OIG
- William McLendon, CompliancePro Solutions
- Elias Nieves, The Health Insurance Store
- Custodia Olivieri, Mednax
- Pam Schulman, Halifax Health
- Suzanne Smeltzer, Greenway Health, LLC
- Rana Tiwari, Rana Tiwari, Attorney-at-law
- Juan Triana, Access Health Care

GEORGIA
- Lourdes Blanche-Sanders, FTI Consulting
- Chris Ideker, Alvarez & Marsal

ILLINOIS
- Paul Brodersen, J Brian Heller, PC
- Jason DeLine, Cigna-HealthSpring
- Diana Eggleston, Olympia Group, LLC
- Heather Hermann, OSF Healthcare
- Trennese Jones, Olympia Group, LLC
- Jeannette King
- Dawn London, University of Chicago Medicine
- Jo-Elle Munchak, Anthem, Inc
- Deanna Perteet, University of Chicago Medicine
- Dianne Pruitt-Scott, University of Chicago Medicine
- Crystal Wiley-Brown, Northwestern University
- Carol Williams, Contractor

INDIANA
- Scott Yahne, Yahne.Law, PC

IOWA
- Aldijana Avdic, University of Iowa Hospitals & Clinics
- Kiley Bybee-Francque, University of Iowa Health Care
- Blessy Peacedale, Marshalltown Medical and Surgical Center

KANSAS
- Juli Wessel, University of Kansas Medical Center

KENTUCKY
- Daniel Blouin, CareSource
- Paula Cissell, CareSource
- Rosmond Dolen, CareSource
- Shanna Sweeney, Procarent

LOUISIANA
- Michelle Brignac, Baton Rouge General Medical Center
- Kerrie Manceaux, Schumacher Group

MAINE
- Michelle Patty, Maine Medical Center
- Shawn Willey, Spectrum Medical Group

MARYLAND
- Lauren Brummell, MedStar Health
- Bonnie Harry, Total Health Care, Inc
- Cecil McCarthy, MedStar Health Inc
- Shelia Merriweather, Park West Health System

MASSACHUSETTS
- Jean Ball, North Shore Medical Center
- Cheryl Field, PointRight Inc
- Lisa Pucci, Cary Medical Center
- Nick Repucci, Boston Children's Hospital
- Robert Rossi, Calloway Laboratories, Inc
- Jesse Shipley, Centene Corporation

MICHIGAN
- Renee Lafata, Karmanos Cancer Center
- Monica Lareau, Trinity Health
- Tammy Salman, VA Ann Arbor Healthcare System
- Audra Smith, Diplomat Pharmacy, Inc
- Sarah Taylor, IHA
- Gayle Wolffis, Beacon Hill at eastgate
- Candace Wood, Spectrum Health

MINNESOTA
- Angela Amore, Fairview Pharmacy Services
- Jill Brown, UnitedHealthcare
- Jennifer DeJoy, St. Jude Medical
- Betty Jo Haggerty, Minneapolis Heart Institute Foundation
- Vanessa Hartzler, Fairview Pharmacy Services, LLC
- Lynn Wieczorek, CentraCare

MISSOURI
- Jaishma Devaiah, Saint Luke's Health System
- James Moran, PwC
- Mitzi Sutton, Mercy Health System
- Teresa Thomas, Mercy Health System

NEVADA
- Carlyn Choate, Department of County Human Services
- Brian Colonna, Renown Health
- Janet Gallegos, Sunrise Hospital and Medical Center
- Melissa Williams, Carson Valley Medical Center

NEW JERSEY
- Barry Munk, Marquis Health Services
- Margery Nathanson, JFK Health System
- Latha Nethula, Rutgers

NEW MEXICO
- Linda Chase, Holy Cross Hospital
- Erin Lagen, Presbyterian Healthcare Services

NEW YORK
- Tina Bowdish, University of Rochester
- Patricia Cooper, National Health Care Associates
- Susan Darlington, Furey, Furey, Leverage, Manzione, Williams & Darlington
- Marie Denis, Long Island Association for AIDS Care, Inc
- Sarah Feder, One Medical Group
- Brad Fuhrman, FTI Consulting
- Mary Glen, University of Vermont Health Network
- Jermel Isaac, Interfaith Medical Center
- David Katz, RC Law Group
- Farah Khakee, Saint Joseph's Medical Center
- Cathleen Krom, Ulster Greene ARC
- Jules Laino, CBLPath Inc
- Jenifer Maynard, Orleans Community Health
- Tina McKiernan, HCCS - A HealthStream Company
- Todd Metcalfe, HCCS - A HealthStream Company
- Doris Nadres, NYU Langone Medical Center
- Darla Rose, Community Health Center of Buffalo, Inc
- Kamlesh Singh, Cardinal McCloskey Community Services

NORTH CAROLINA
- Deborah Borawski, Northern Hosp of Surry County
- Bryan Burnette, Community CarePartners, Inc
- Lisa Dennis
- Nancy Oldham, OptiCare Managed Vision, Inc

NORTH DAKOTA
- Diane Doria, Trinityhealth

OHIO
- Kimberly Baughman, Wood County Hospital
- Rebecca Benston, CareSource
- Christy Conway, Dayton Children's Hospital
- Tamara Gump, Mary Rutan Hospital
- Tina Hayes, Berger Health
- Lauren Krasnodembski, Cardinal Health
- Malila Nguyen, Nationwide Children's Hospital
- Cheryle Swartz, CareSource
- Sean Woodson, CareSource

OKLAHOMA
- Michelle Crissup, OSU Center for Health Sciences
- Christine Peterson, Parkside, Inc

OREGON
- Jeremy Ainsworth, PT Northwest
- Mindi Burdick, WVP Health Authority
- Denise Butler, PeaceHealth
- Peter Charlton, Ricochet Partners
- Dee Dee Haggard, Columbia Memorial Hospital
- Jeanne McKirchy, Ricochet Partners
- Kristal Miller, WVP Health Authority
- Nina Salzman, Providence Health Systems
- Carrie Smith, Providence Health Plan

PENNSYLVANIA
- Denise Barger, Benchmark Risk Management
- Elizabeth Gaffney, Onix Group
- Shelly Hepler, Erie VA Medical Center
- Denise Kruse, Susquehanna Health
- Lori Mahan, Main Line HealthCare
- Patricia Neumann, ECRI Institute
- Lynne Oliveri, The Children's Hospital of Philadelphia
- Renee Peterson, Compassionate Care Hospice
- Nirmala Thevathasan, Huron Consulting Group

SOUTH CAROLINA
- Courtney Cable, Advicare
- Ruth Cummins, BlueCross BlueShield of South Carolina

SOUTH DAKOTA
- Sandie Mulder, Dow Rummel Village

TENNESSEE
- Christina Cannon, Mental Health Cooperative Inc
- Janet Jones, Community Health Systems
- Christopher Moore, Results Physiotherapy
- Amy Van Fleet, LifePoint Hospitals Inc
- Sean Weiss, DoctorsManagement LLC
- Holly West, Cigna-HealthSpring

TEXAS
- Cherie Batsel, Law Office of Cherie K Batsel
- Deepika Bhatia, University of Texas Southwestern
- Janice Drury, Global Healthcare Alliance
- Judy Dunnahoe, Oncology Consultants
- Carol Dzierski, Bay Area Regional Medical Center
- Lindsey Estep, Baylor Scott & White Health
- Jennifer Gibbons-Ramirez, Baylor Scott & White Health
- Paula Griffith, JPS Health Network
- Abel Guevara
- Aju Koshy, ConvergePoint
- Angela Lairson, Pacific Labs
- Michelle Leacock, Cardiovascular Provider Resources
- Annette Lee, Cigna-HealthSpring
- Cristina Loayza, PreCheck Inc
- Nancy Logan Jarrar, Baylor College of Medicine
- Abiya Malhotra, Texas FSED LLC
- Sean McKenna, Haynes and Boone, LLP
- Samantha Meadors, Epic Health Services, Inc
- Natalie Moya, Texas Childrens Hospital
- Janette Nguyen, MRC - Medical Research Consultants
- Jeffrey Scribner
- Kathy Stevenson, Cigna HealthSpring
- Melissa Stokes, Pacific Labs
- Jerel Sukarangsan, Oncology Consultants
- Linda Ward-Graves, Texas Children's Hospital
- Gretchen Watson, MRC - Medical Research Consultants
- Cheryl Young, HealthTexas Provider Network

UTAH
- Stephanie Cecchini, Aviacode
- Dana Frederiksen, University of Utah
- Aja Ogzewalla, Medical Review Institute of America, Inc

VIRGINIA
- William Davis, Grafton Integrated Health Network
- Mary Evans, Golden Living
- Ernestine Fuller, DCS Corp
- Michelle Kidwell, Grafton Integrated Health Network
- Mary Potter, Carilion Clinic
- Angela Simmons, Total Medical Compliance
- Deana Wilder, UIC Technical Services LLC
- Edward Working, Veterans Health Administration

WASHINGTON
- Beth Aaron, Providence Health & Services
- Kelly Di Loreto, MultiCare Health System
- Margaret Griffiths, Qualis Health
- Timothy Reed, Yakima Valley Memorial Hospital
- Eva Samtmann, Sound Urological Associates
- Jennifer Svoboda, Prestige Care, Inc
- Karen Westenberger, Molecular Testing Labs

WISCONSIN
- Kerry Chase, PharmaSeek Financial Services
- Tiffany Faber, Security Health Plan
- Margaret Fischbach, Milwaukee Center for Independence
- Jennifer Grant, Childrens Hospital of Wisconsin
- Cathy Lacenski, Forefront Dermatology Management, LLC
- Sarah Pitsoulakis, Milwaukee Center for Independance
- Megan Tenboer, PharmaSeek Financial Services

WASHINGTON DC
- Peter Dressel, FTI Consulting
- Deborah Gairbay, GW Medical Faculty Associates

PUERTO RICO
- Maria Fullana-Hernandez
- Antonio Marrero, HMI, Inc
- Dagmar Medina, TriServe Tech
- Verónica Ramos-Vera, Centros Integrados de Servicios de Salud de Lares y Quebradillas
- Nancy Santana-Vélez, TriServe Tech
- Vanessa Viera

CANADA
- Leah Stansbury, PointClickCare

JOIN HCCA
ON SOCIAL MEDIA

www.hcca-info.org

Takeaways

July 2015

Compliance TODAY

Tear out this page and keep for reference, or share with a colleague. Visit www.hcca-info.org for more information.

When risk assessments become exhibits: Are you prepared?

Michael J. McCarthy and Andrew W. Mahler (page 27)

- Patients whose protected health information (PHI) has been breached are successfully suing providers in state courts.
- These lawsuits are usually based on claims that the provider negligently handled PHI, using HIPAA as the standard of care providers owe their patients.
- Schedule meetings with the appropriate people in your organization to discuss new legal trends.
- Change your perspective when writing risk assessments or incident reports—they could become exhibits in a lawsuit.
- Get input and counsel from others in your organization, such as the Office of General Counsel, when you have to make a tough call.

RAC forecast: Are we in the eye of the storm or are sunny skies ahead?

Isabella R. Edmundson and Lauren S. Gennett (page 33)

- The RAC program has been in a lull since June 2014, and the award of the new Medicare Part A/B RACs has been delayed due to a pre-award protest.
- On December 30, 2014, CMS announced several program changes aimed at reducing provider burden and increasing transparency in the RAC program.
- Some of these program changes may be beneficial, but much depends on how CMS will implement and enforce the changes.
- The changes will not be implemented until the new RAC contracts are awarded, which for certain contracts may not be until at least 2016.
- Providers should prepare for RAC reviews to begin again in full force once RACs are able to resume regular reviews, including patient status reviews.

Compliance tips: Evaluate your effectiveness by asking 50 questions

Shelly L. Harris (page 43)

- Build awareness and effectiveness by asking the right questions.
- Apply the answers to the annual risk assessment and work plan.
- Create metrics based on questions.
- Assess the tone and climate of an organization.
- Completing a small employee survey can help evaluate effectiveness.

The Two-Midnight Rule: Past, present, and future *[UPDATE]*

Janice Anderson and Sara Iams (page 47)

- The Two-Midnight Rule is highly controversial and its future is questionable.
- Since the adoption of the Two-Midnight Rule, CMS enacted a Probe & Educate program and delayed RAC enforcement of the Two-Midnight Rule, in large part due to push-back from the industry.
- The deadline that would trigger RAC enforcement of the Two-Midnight Rule has been extended several times, most recently through September 30, 2015.
- The Medicare Payment Advisory Commission (MedPac) also is not favorable to the Two-Midnight Rule and recommended withdrawal of the Rule.
- In the 2016 proposed Inpatient Prospective Payment System (IPPS) rule, CMS indicated that it would consider the MedPac recommendations in its rule-making related to the 2016 proposed Outpatient Prospective Payment System rule to be released this summer.

Whip your incident response program into shape

Nadia Fahim-Koster (page 51)

- Understand requirements behind an incident response program (IRP).
- Identify the different components of an effective IRP.
- Learn how to prepare for your testing exercise.
- Learn how to develop meaningful testing scenarios.
- Understand how to conduct and document the testing.

Decreasing the chances of extensive, costly OCR audits

Virginia Sizemore and Chris Luoma (page 57)

- All hospitals must now have business associate (BA) agreements in place.
- Hospitals with multiple violations could face $6 million in fines.
- The first step is understanding the risks represented by BAs.
- Every company paid within past 24 months should be examined.
- If audited, hospitals should send only the information requested.

Surveys— Paper, electronic, or both?

Paul P. Jesep (page 61)

- Paper surveys still have great value to an organization.
- Do not replace surveys with online tools. Leverage paper surveys as tools.
- A paper survey lends itself to sensitive information by providing more anonymity.
- Paper surveys give the compliance officer another opportunity to directly engage with staff.
- The effort taken to compile and analyze data from paper and online surveys is still a wise investment.

Creating effective solutions for data privacy concerns in clinically integrated networks

Janice Anderson and Ken Briggs (page 63)

- Clinically integrated networks are becoming the cornerstone of the healthcare delivery system.
- Privacy laws pose complex and contradictory hurdles for successful integration.
- Data exchange through networks has significant liability and regulatory implications.
- Certain structures of clinically integrated networks are more effective than others.
- Networks should investigate different options to structure the network in light of applicable state and federal privacy laws to determine the most efficient solution.

The lure of Part D reimbursement: Should dentists fish or cut bait?

Jon H. Klein (page 69)

- Review provider contracts in response to legislative changes.
- Dialogue with non-compliance staffers to assess impacts of new legislation.
- Monitoring efforts include matching NPI code numbers to the treating physician.
- Know risks associated with patient surcharges and co-pays.
- Cross-train in dental/medical for compliance staff involved in integrated care.

Compliance 101: The seven essential elements, Part 5: Reporting & investigation

Adam K. Weinstein, Cindy Hart, and Walter E. Johnson (page 72)

- Diverse personality types, comfort levels, and belief systems may determine how an employee prefers to report a problem or concern.
- Offering several reporting channels may increase the number of problems or concerns reported.
- Onsite visits and regular communication may improve comfort levels of employees, thereby increasing the number of problems or concerns reported.
- Investigating reported problems or concerns reinforces the compliance message that reporting is encouraged.
- Employees participating in investigations may become more cognizant of the compliance program and decide to identify their preferred reporting channel.

HCCA's Upcoming Events

Learn more about HCCA's educational opportunities at www.hcca-info.org/events

July 2015

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
			1	2	3 HCCA OFFICE CLOSED	4 *Independence Day*
5	6	7	8	9	10	11
12	WEB CONFERENCE 13 *Examining Physician Compensation Arrangements*	14	15	WEB CONFERENCE 16 *Mitigating Risk in the Revenue Cycle: Breaking the Code in the Appropriate Patient Status*	17 *Eid al-Fitr (Ramadan Ends)*	18
19	WEB CONFERENCE 20 *How to Prepare for an OCR Compliance Audit*	WEB CONFERENCE 21 *Long Term Care Hot Topics in Compliance*	WEB CONFERENCE 22 *Aligning Your Research Compliance Work Plan with the Unrecognized Risks of Conducting Human Research*	WEB CONFERENCE 23 *Millennials in Compliance: Technology and Social Demographics Driving Agile Compliance*	24	25
26	27	WEB CONFERENCE 28 *What All Healthcare Entities Should Know About CMS Guidance for an "Effective Compliance Program"*	WEB CONFERENCE 29 *Embracing Quality: One Institution's Approach to Managing Compliance Risks*	30	31	

August 2015

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
						1
2	3	4	WEB CONFERENCE 5 *Emerging CDI Trends in 2015: CDI Survey Findings and Tips to Elevate Physician Engagement*	6	7	8
9	10 **Healthcare Basic Compliance Academy** New York, NY	11	12	WEB CONFERENCE 13 *The Role for Coders within the Private Physician Practice* CHC Exam	14	15
16	17	18	19	20	21	22
23	24	25	26	WEB CONFERENCE 27 *Compliance and Managing the EMR Risks*	28	29
30	31					

Basic Compliance Academies

August 10–13 • New York, NY — **SOLD OUT**
September 14–17 • Chicago, IL — **LIMITED SEATS**
September 28–October 1 • Scottsdale, AZ
October 19–22 • Las Vegas, NV
October 26–29 • Nashville, TN
November 16–19 • Orlando, FL
Nov 30–Dec 3 • San Diego, CA

Regional Conferences

September 11 • Boston, MA
September 18 • Minneapolis, MN
September 25 • Overland Park, KS
October 2 • Indianapolis, IN
October 9 • Pittsburgh, PA
October 15–16 • Honolulu, HI
October 23 • Denver, CO
November 6 • Louisville, KY
November 13 • Scottsdale, AZ
November 20 • Nashville, TN
December 4 • San Francisco, CA
December 11 • Houston, TX

Clinical Practice Compliance Conference

October 11–13 • Philadelphia, PA

Healthcare Enforcement Compliance Institute

October 25–28 • Washington DC

Healthcare Privacy Basic Compliance Academies

November 2–5 • Orlando, FL

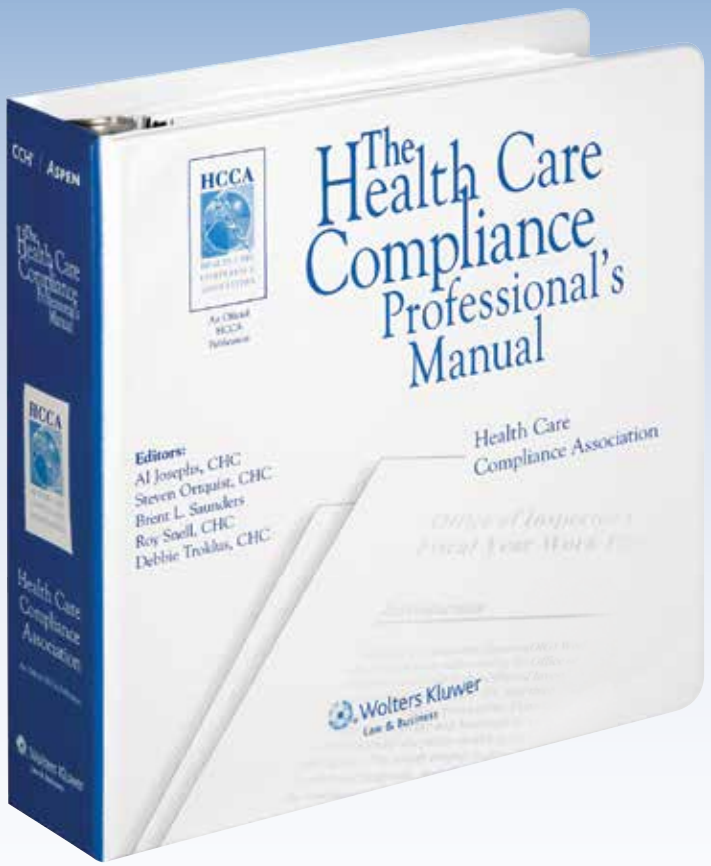
Research Basic Compliance Academies

November 2–5 • Orlando, FL

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Dates and locations are subject to change.

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: $419
NON-MEMBER PRICE: $459

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

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

Wolters Kluwer
Law & Business

NEW *from HCCA in 2015*

Register by August 18

SAVE $175

Healthcare Enforcement Compliance Institute

OCTOBER 25–28, 2015 | WASHINGTON HILTON | WASHINGTON DC

General Session speakers announced

Michael Horowitz
Inspector General, United States Department of Justice

Cynthia Schnedar
Director, Office of Compliance, FDA's Center for Drug Evaluation and Research

Greg Demske
Chief Counsel to the Inspector General, HHS-OIG

Jocelyn Samuels
Director, U.S. Department of Health and Human Services, Office for Civil Rights

Learn more at hcca-info.org/heci

Questions? taci.tolzman@corporatecompliance.org

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION