HCCA HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

March 2015

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

Protecting the healthcare rights of everyday citizens

an interview with Jocelyn Samuels

Director of the Office for Civil Rights, U.S. Department of Health & Human Services

See page 18

NEW
from HCCA
in 2015

Register by August 18

SAVE $175

Healthcare Enforcement Compliance Institute

October 25–28, 2015 | Washington Hilton | Washington DC

HCCA's Healthcare Enforcement Compliance Institute gives you the opportunity to learn best and leading-edge practices for the compliance lawyer.

Go beyond legal analysis, learn how to implement systems that ensure the law is followed, and gain practical advice from experts in a one-of-a-kind forum where lawyers and compliance officers work together.

- Discover and discuss the latest trends in regulatory changes.
- Hear the latest legal analysis, and learn what you need to do to ensure you're working most efficiently and in compliance with all the regulations.
- Learn from legal experts dedicated to sharing the latest and best practices for implementing an effective compliance program that finds and fixes problems.

Learn more at hcca-info.org

Questions? taci.tolzman@corporatecompliance.org

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

by Roy Snell, CHC, CCEP-F

Jeff Foxworthy, Compliance, and Internal Audit

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

Jeff Foxworthy did a comedy bit called "You might be a redneck if…"

- "…you ever cut your grass and found a car."
- "…you think the stock market has a fence around it."
- "…your wife has ever said, 'Come move this transmission so I can take a bath.'"

Snell

Using Foxworthy's bit, I have developed some "You might not have a compliance program if the Chief Compliance Officer…" (Unfortunately, these are not even remotely funny.)

- …can't report material unresolved issues to the audit committee.
- …can't report material compliance plan impediments to the audit committee.
- …annual review is done by someone they occasionally have to investigate.
- …isn't responsible for all elements of a compliance program.
- …isn't responsible for all risk areas.
- …can't investigate something they deem necessary to investigate.
- …doesn't have access to people or information they need access to.

It is tough to get all these things in place. We are going through a progression. It will improve. But it's misleading to call someone a Chief Compliance Officer if they are not performing the essential elements of the job. You can't call something a compliance failure if you fail to have an effective Chief Compliance Officer.

> …it's misleading to call someone a Chief Compliance Officer if they are not performing the essential elements of the job.

It is no different for Internal Audit. "You might not be an internal auditor if…"

- …your annual review is completed by the people you audit.
- …you don't have access to the audit committee of the board.
- …you can't report all unresolvable and material audit findings issues to the board.
- …you can be prevented from accessing people or information necessary to do your job.

Contents

March 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).

> OCR is committed to implementing an effective audit program, and [HIPAA] audits are an important compliance tool.

See page 22

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 3

ERC study: Employee views of leaders' personal conduct drives perceptions of their ethical leadership

According to the Ethics Resource Center (ERC) study, "Ethical Leadership: Every Leader Sets a Tone," "Corporate leaders who are perceived by their employees as demonstrating strong personal character are much more likely to be perceived as setting a strong tone from the top."

The ERC press release on the research noted, "The most significant factor in ethical leadership is personal character. Drawing on detailed analysis of data collected as part of its National Business Ethics Survey (NBES), ERC also found that employees in every size of company judge leaders primarily on the same three factors - character as experienced through interactions, how they handle crises and the policies and procedures leaders establish to manage the company."

ERC "recommended that companies that want to support strong ethical leadership should:

- Seek out personal character when hiring and make 24-7 integrity a job expectation.
- Educate managers about the way employees evaluate leaders
- Encourage leaders to share credit for success and seek honest feedback from employees.
- Annually review business objectives and policies to ensure they promote ethical performance."

For more: *http://bit.ly/23DYdWH*

Top fraud and corruption trends for 2015

Ernst & Young (EY) Fraud Investigation & Dispute Services (FIDS) recently released its "Top Fraud and Corruption Trends for 2015." According to EY, the 2015 top trends are highlighted "by a dramatic rise in cyber security risk across all industries. Bribery and corruption too will challenge organizations and their Boards, especially in highly regulated industries such as financial services and life sciences, as they look to develop new approaches to mitigate these risks while balancing demands for global growth."

The EY press released noted that its Fraud Investigations & Dispute Services (FIDS) has identified the five key themes listed below which "companies should incorporate in their planning in 2015."

1. Cyber readiness is challenging the C-Suite and Boards
2. Increased focus on Foreign Corrupt Practices Act (FCPA) enforcement actions against individuals
3. Use of Forensic Data Analytics (FDA) in anti-bribery/anti-corruption monitoring and investigations
4. Regulated industries: Financial Services
5. Regulated industries: Life Sciences & Healthcare

For more: *http://bit.ly/2yhnm4e*

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

Regulatory news

Hospital Value-Based Purchasing Program—FY 2015

According to a recent Centers for Medicare and Medicaid Services (CMS) fact sheet, the Hospital Value-Based Purchasing (VBP) Program "adjusts payments to hospitals under the Inpatient Prospective Payment System (IPPS) based on the quality of care they furnish to patients. For FY 2015, as directed by the law, CMS increased the applicable percent reduction, the portion of Medicare payments available to fund the value-based incentive payments under the program, from 1.25 to 1.5 percent of the base operating DRG payment amounts to all participating hospitals. CMS estimates that the total amount available for value-based incentive payments in FY 2015 will be approximately $1.4 billion.

"The Hospital VBP Program provides a useful snapshot of how hospitals are performing on important quality indicators of patient care, quality, efficiency, and well-being and is one of many Affordable Care Act programs Medicare is implementing to pay for quality instead of quantity. The domains for FY 2015 were:

- Clinical Process of Care: 20 percent
- Patient Experience of Care (HCAHPS survey): 30 percent
- Outcome (hospital mortality measures for acute myocardial infarction, heart failure, and pneumonia, and the central line-associated bloodstream infection measure): 30 percent
- Efficiency (Medicare Spending per Beneficiary measure gauges efficiency by calculating total cost to Medicare for hospitals' episodes): 20 percent."

According to the CMS, the agency "has posted Hospital Value-Based Purchasing incentive payment adjustment factors for fiscal year 2015 on the CMS website." The Hospital VBP Program adjustment factors are available at http://bit.ly/HospVBP.

"Depending on how well hospitals measured up to their peers on important health-care quality measures during a prior performance period, and on how much they improved over their own historical performance, they will be paid more or less for each Medicare fee-for-service discharge in fiscal year 2015 than they would have been paid in the absence of this program."

For more:
http://bit.ly/2014HBVPFact

To see the FY 2015 value-based incentive payment adjustment factors:
http://bit.ly/2015VBIFact

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

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

SCCE/HCCA 2014–2015 BOARD OF DIRECTORS

EXECUTIVE COMMITTEE

Gabriel L. Imperato, Esq., CHC
SCCE/HCCA President
Managing Partner, Broad and Cassel, Fort Lauderdale, FL

Sara Kay Wheeler, JD, CHC
SCCE/HCCA Vice President
Partner, Attorney at Law, King & Spalding, Atlanta, GA

Urton Anderson, PhD, CCEP
SCCE/HCCA Second Vice President
Director, Von Allmen School of Accountancy, Gatton College of Business and Economics, University of Kentucky, Lexington, KY

Margaret Hambleton, MBA, CHC, CHPC
SCCE/HCCA Treasurer
Vice President, Chief Compliance Officer, Dignity Health, Pasadena, CA

Lori Strauss, RN, MSA, CPC, CHC, CHPC, CCEP
SCCE/HCCA Secretary
Chief Corporate Compliance & Privacy Officer, University of Virginia Health System, Charlottesville, VA

Art Weiss, JD, CCEP-F, CCEP-I
SCCE/HCCA Non-Officer Board Member
Chief Compliance & Ethics Officer, TAMKO Building Products, Joplin, MO

John Falcetano, CHC-F, CHRC, CHPC, CCEP-F, CCEP-I, CIA, CICA
SCCE/HCCA Immediate Past President
Chief Audit/Compliance Officer, Vidant Health, Greenville, NC

EX-OFFICIO EXECUTIVE COMMITTEE

Roy Snell, CHC, CCEP-F
Chief Executive Officer, SCCE/HCCA, Minneapolis, MN

Stephen Warch, JD
SCCE/HCCA General Counsel | Nilan Johnson Lewis, PA, Minneapolis, MN

BOARD MEMBERS

Andrijana Bergant, CCEP-I
Advisor of the Compliance and Integrity Centre, NLB, Ljubljana, Slovenia

Shawn Y. DeGroot, CHC-F, CHRC, CHPC, CCEP
Associate Director, Navigant Consulting, Denver, CO

Marjorie Doyle, JD, CCEP-F, CCEP-I
Principal, Marjorie Doyle & Associates, Landenberg, PA

Odell Guyton, CCEP, CCEP-I
Vice President Global Compliance, Jabil, St. Petersburg, FL

Debra Hinson, MBA, RRT-NPP, CHC, CHP, CHRC, CCEP
Chief Research & Privacy Compliance Officer, Columbus Regional Health, Columbus, GA

Shin Jae Kim, CCEP, CCEP-I
Partner, TozziniFreire Advogados, São Paulo, Brazil

Joseph Murphy, JD, CCEP, CCEP-I
Senior Advisor, Compliance Strategists, New Providence, NJ

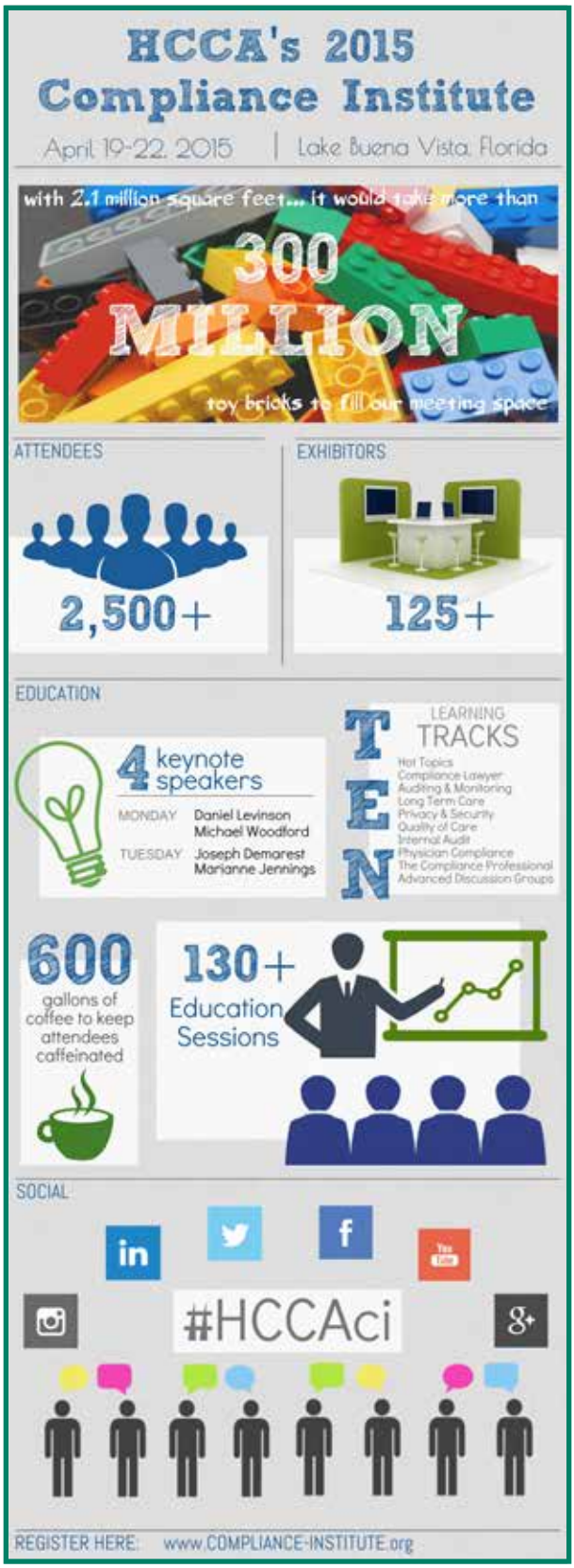
Jenny O'Brien, JD, CHC, CHPC
Chief Compliance Officer, UnitedHealthcare, Minnetonka, MN

Daniel Roach, JD
General Counsel and Chief Compliance Officer, Optum360, Eden Prairie, MN

Debbie Troklus, CHC-F, CHRC, CHPC, CCEP-F, CCEP-I
Managing Director, Aegis Compliance and Ethics Center, Chicago, IL

Sheryl Vacca, CHC-F, CHRC, CHPC, CCEP-F, CCEP-I
Senior Vice President / Chief Compliance and Audit Officer, University of California, Oakland, CA

Infographic of the month



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

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

March 6 • St Louis, MO

March 13 • Washington DC

March 20 • Charleston, SC NEW

April 30–May 1 • San Juan, PR

May 8 • Columbus, OH

May 15 • New York, NY

June 5 • Philadelphia, PA

June 12 • Seattle, WA

June 19 • Santa Ana, CA

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

HCCA *conference news*

19th Annual Compliance Institute

April 19–22, 2015 | Lake Buena Vista, FL

www.compliance-institute.org

Don't miss the annual Compliance Institute, HCCA's largest event. Over the course of four days, you have the opportunity to attend a variety of sessions covering topics such as:

- Healthcare reform
- Hospital physician alignment
- Compliance effectiveness
- HIPAA privacy/data breach

The 2015 Compliance Institute offers 10 tracks:

- Internal Audit — *new this year*
- General Compliance & Hot Topics
- Long-Term Care
- Privacy & Security
- Physician Compliance
- Compliance Lawyer
- Auditing & Monitoring
- How to Succeed as a Compliance Professional
- Quality of Care
- Advanced Discussion Groups

And don't miss hearing from keynote speakers:

- Daniel Levinson, Inspector General, HHS
- Michael Woodford, Whistleblower and Former Global CEO of Olympus
- Joseph Demarest, Assistant Director, Cyber Division, FBI
- Marianne Jennings, Ethicist

The full agenda is available online at *www.compliance-institute.org*. Register between March 1–31, 2015 and receive a free copy of the book *501 Ideas for Your Compliance and Ethics Program* by Joseph E. Murphy.

Here are highlights of just a couple of the educational sessions offered:

SESSION 601: Tue, April 21, 1:00–2:00 pm

Compliance post-Affordable Care Act: Even more important?

Sean McKenna, *Partner, Haynes and Boone, LLP*

Kenneth Zeko, *Director, Navigant*

Bret Bissey, *Senior VP Compliance Services, MediTract, Inc.*

QUESTION: Does compliance matter post-Affordable Care Act?

ANSWER: More than ever.

Our session will provide three perspectives why compliance is critical and will remain so for years to come. Hear from a former chief compliance officer who lived under mandated integrity obligations, a national consultant who spends every day helping providers with compliance issues, and a former OIG and DOJ attorney who handled compliance investigations first-hand and saw good, bad, and non-existent compliance efforts.

SESSION W18: Wed, April 22, 10:00–11:45 am

Extrapolation: Understanding the statistics — and what to do when it happens to your audit results

Andrea C. Merritt, *Partner, Athena Compliance Partners*

Frank C. Castronova, *Health Care Management Biostatistician, BCBS of Michigan*

You have been selected to be audited. But now you ask, "What sampling methods are being used and are they correct? How and why are my audit findings going to be extrapolated? What can I do when my results are extrapolated?" Ease your fears and find answers to all of your questions by attending this session.

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 | My Account | Events | Add CEUs

Number of website visits last month

44,104

Updating your profile

The *My Account* section of the HCCA website is a great way to keep track of your certifications, CEU information, and registrations for upcoming events, but it's also where you can update your biography and picture—which are what will be used if you decide to speak at any of our conferences.

To change any of your information, log in at *www.hcca-info.org*, click *My Account*, then *Update Bio*. You can also update your picture in either the *My Account* or *Update Bio* pages, by clicking *Change Picture*. (Filetypes: jpg, png, and bmp; size limit: 160px.)

Video of the month

What are the benefits of self-disclosure?

http://bit.ly/votm-2015-03

Upcoming HCCA Web Conferences

3/3	• Increase Your Value through HIPAA Education
3/5	• Preparing Your Organization for Round Two: Tips for Surviving Privacy & Security Desk Audits
3/11	• Patient and Data Privacy Considerations in a Private Health Information Exchange
3/16	• Settling False Claims Act Cases with the Federal Government
3/18	• Medical Necessity Compliance and the Two-Midnight Rule
3/30	• Internal Compliance Surveys: Measuring Your Department's Effectiveness

LEARN MORE AND REGISTER AT

www.hcca-info.org/webconferences

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 18,800 members, our LinkedIn group fosters more than 75 new discussion posts every week. Some recent highlights:

Home Health Care Policies: Medicare Spending Slows Down Below Expectations
Melissa Cott

No Pre-Existing Condition Exclusions Means HIPAA Certificates No Longer Required http://ow.ly/GEbdx
Kortney Nordrum

Are you paying attention to your BA's compliance?
Chris Apgar, CISSP
CEO & President

Millennials want PHR on the go
Tom Corall
Healthcare Consultant at iPractice Healthcare [LION]

Good info on media sanitization from NIST.
Frank Ruelas
HIPAA College

Pinterest — *www.pinterest.com/theHCCA*

Check out our Pinterest boards for HIPAA, ICD-10, ACA, Compliance Videos, and using Technology & Social Media in healthcare. Our "infographics of the month" and much more can all be found on our boards.

HCCA*net*® — *www.hcca-info.org/HCCAnet*

HCCA's own social network. Signing up is free and you'll be able to network, ask and answer questions, and collaborate with your healthcare compliance peers.

SlideShare — *www.slideshare.net/theHCCA*

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

Twitter — *www.twitter.com/theHCCA*

Join 10,700+ others and follow HCCA for breaking news and insights. Recent favorite tweets:

Facebook — *www.facebook.com/hcca*

We're on Facebook, too! "Like" our page for healthcare compliance news and networking. Some recent posts include:

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

PEOPLE *on the* MOVE

▶ Actavis plc, a global specialty pharmaceutical company with U.S. headquarters in Parsippany, NJ, announced that **Jonathon Kellerman** has joined the company as Executive Vice President, Global Chief Compliance Officer. Mr. Kellerman is a member of the Actavis Executive Leadership Team and will report directly to Brent Saunders, CEO and President.

▶ **Tammy Preisner** has been named Chief Compliance Officer for Evariant in Farmington, CT.

▶ FirstCare Health Plans in Austin, TX has named **Sonya Henderson** as the new Vice President of Compliance and Government Programs.

▶ **Alejandra (Alex) Clyde**, MHA, CHC, has been named Compliance Officer for Health Plan of San Joaquin, in French Camp, CA.

▶ **Sara Tubbs**, MBA, LBSW, has joined Midwest Compliance Associates as a consultant in Cedar Falls, IA.

▶ ConnectYourCare, in Hunt Valley, MD, has named **Julie M. Linn** as the company's new Chief Compliance Officer.

▶ **Jennifer Wilkinson** is now working in the position of Compliance at Community Health Programs, Federally Qualified Health Center in Great Barrington, MA.

▶ Sierra Providence Health Network, in El Paso, TX, recently announced it has promoted **Alma Terrazas** to Market 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

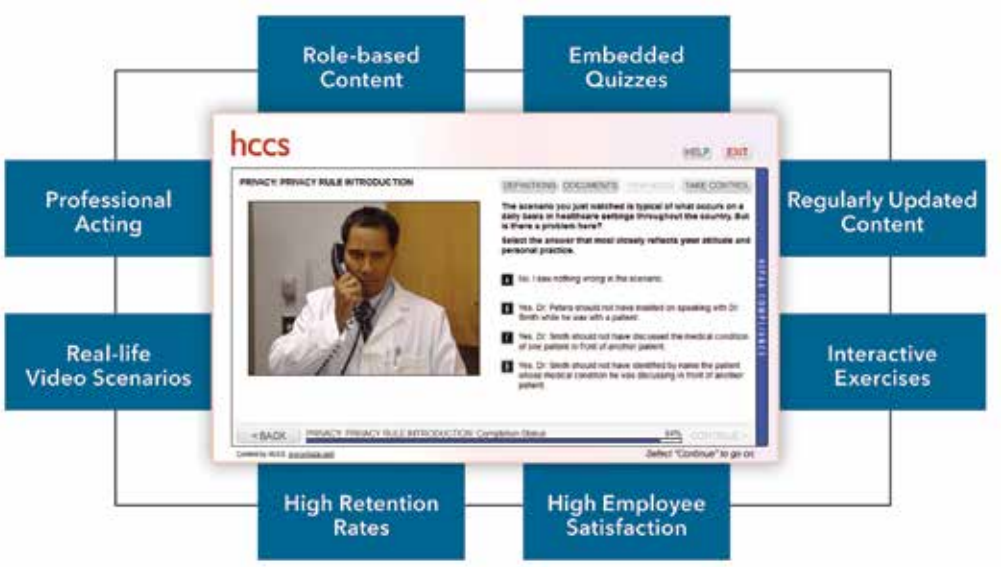
General Compliance Suite

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

Jocelyn Samuels
Director of the Office for Civil Rights,
U.S. Department of Health & Human Services,
Washington DC

an interview by Erika M. Bol, CHC, CHPC, CIPP/US

Meet Jocelyn Samuels

Erika M. Bol *(erika.bol@anthem.com), Director, Corporate Privacy – Incident Program for Anthem, Inc. in Denver, conducted this interview with* ***Jocelyn Samuels*** *in December 2014.*

EB: Your previous position was as the Acting Assistant Attorney General for Civil Rights at the U.S. Department of Justice. You are a veteran federal civil rights official and litigator who has been actively engaged in legislative and policy advocacy to promote enforcement of Title VII of the Civil Rights Act of 1964 and Title IX of the Education Amendments of 1972. You worked as Labor Counsel to the late U.S. Senator Edward M. Kennedy and as a Senior Policy Attorney at the Equal Employment Opportunity Commission (EEOC). Was it always your plan to spend your career working for the government or did you simply "fall" into government work?

JS: I believe most civil rights lawyers share a common commitment to creating a just society through legal means. As a result, many of us find ourselves in government service, where we can help to bring about change in a systemic and significant way. Public service is wonderfully fulfilling, and I feel lucky to have the opportunity to do it. Every day you can work to make meaningful changes in the lives of the people you serve. Every day presents new challenges, along with multiple opportunities to improve the health and well-being of people across the nation. It's been very rewarding, and I am so excited to be at the HHS Office for Civil Rights, where we protect individuals' fundamental rights to participate in important

healthcare and human services programs without facing unlawful discrimination, and ensure that individuals enjoy strong protections for health information privacy and security.

EB: You come to HHS/OCR at a time when enforcement of HIPAA, the federal law governing patients' medical privacy, is at an all-time high. How do you see your background in enforcing civil rights laws as helping to shape the HIPAA program going forward?

JS: While my background has focused on enforcement of the laws banning discrimination based on race, sex, national origin, religion, age, and disability, work to enforce HIPAA and individuals' rights to the privacy and security of their health information falls squarely into the great civil rights tradition. In each case, it is critical to ensure that individuals are treated fairly in their interactions with institutions and that those institutions respect the rights conferred by law on the people with whom they come in contact. Enforcement requires that those subject to these laws be held accountable for compliance and, where necessary, that corrective actions or other remedies be taken for non-compliance. Under both HIPAA and civil rights laws, we ensure that individuals are aware of their rights and that people and organizations subject to the laws have the tools and guidance they need to understand their obligations. At OCR, we will continue to use these principles to run a strong and effective HIPAA compliance program.

Listening sessions with key stakeholders across the country are vitally important to ensure that we are… hearing… about what is working in practice, and about the challenges they are facing in their efforts to ensure HIPAA compliance.

EB: Many privacy officers speak highly of meeting you during your meet-and-greet sessions, which you held and attended across the nation. What was the purpose of these sessions, and did they achieve the objectives that you wanted?

JS: Listening sessions with key stakeholders across the country are vitally important to ensure that we are connecting with and hearing from the healthcare industry about their top priorities, about what is working in practice, and about the challenges they are facing in their efforts to ensure HIPAA compliance. During these sessions, I heard firsthand about emerging issues and about some of the areas in which OCR should be considering additional guidance and technical assistance. The initial meet-and-greet sessions I held in our regional offices across the country were exceptionally productive and informative, and I look forward both to continuing those dialogues and to expanding the discussions to more stakeholders in the coming months.

EB: In at least one of your meet-and-greet sessions, the concept of a government-initiated task force made up of chief privacy officials from around the country was discussed, the idea being for industry representatives to come together, brainstorm, and provide advice to government regulators on what will and will not resonate in their respective industries (e.g., large providers, health plans, small group practices, etc.). This kind of collaboration is

currently working well with cybersecurity initiatives. Do you ever envision such a forum or committee dealing with HIPAA initiatives?

JS: Within the healthcare industry, chief privacy officers have important firsthand knowledge about implementation of and compliance with the HIPAA Rules, which is why we made sure to include them in our regional listening sessions. We are always looking for new ways to engage with and learn from these critical stakeholders and will utilize all of the options available to us to ensure that we are providing the best guidance to the industry.

EB: It is obvious from your career achievements that you are passionate about ensuring and protecting the rights of citizens, including working with individuals who have developmental disabilities, promoting student diversity, and preventing discrimination in housing, lending, and employment. How do you see OCR reaching new heights in the areas of patients' rights to access their health records and increased involvement in their medical care?

JS: Through OCR's work to ensure that individuals have access to their health information, I see the importance of HIPAA on a daily basis. Many individuals want to play a more active role in their healthcare; they are empowered to do so when they can gain access to their health records. Indeed, access to health records is the critical initial building block in enabling individuals to take more control of their healthcare decision-making—which is, in turn, an essential element of improving health outcomes.

In the last several years, OCR has done significant work in this area, including making changes to the HIPAA Rules to strengthen individuals' rights to receive an electronic copy of their health information and to access their test reports held by laboratories.

Further, OCR has made tremendous progress helping patients understand and exercise their rights to access their health records under HIPAA. For example, OCR published a series of 10 videos on *YouTube* explaining patients' rights under HIPAA—including one dedicated entirely to the right of access—which have received almost 2 million views.

Working with our partners in the HHS Office of the National Coordinator for Health Information Technology, we developed Model Notices of Privacy Practices. These notices, which have been downloaded more than 200,000 times, are outstanding plain-language tools available in both English and Spanish for healthcare providers and health plans to use to educate their patients about their rights to their health information.

We also implemented our *Information is Powerful Medicine* campaign (http://aids.gov/privacy), which is a highly successful example of how we can educate and empower consumers to take charge of their healthcare by accessing their health information.

I will continue to build upon these successes to ensure that individuals know about their right to access their information.

EB: If you had to pick the one critical thing covered entities and business associates should ensure they are doing and documenting to be in compliance with HIPAA's Privacy, Breach, and Security Rules, what would it be?

JS: Based on our enforcement experience and the breach reports we've received, it is critical that entities take a comprehensive and thorough approach to assessing and addressing the risks to all of the protected health information (PHI) they maintain. In addition, covered entities should ensure that they not only have comprehensive policies and procedures for compliance with the HIPAA Rules, but also that the policies and procedures are being clearly communicated to, and implemented appropriately by, workforce members.

EB: As witnessed by large breach reports to OCR, safeguarding PHI on mobile devices

continues to be a challenge for many healthcare organizations. Do you envision that OCR may mandate encryption on mobile devices in the future to safeguard individuals' PHI when these devices are lost or stolen?

JS: The HIPAA Security Rule requires covered entities and business associates to implement reasonable and appropriate safeguards to protect electronic identifiable health information, and encryption is an effective control to prevent unauthorized access. While we understand that encryption may not be a practical solution for all entities, in all settings, to protect electronic PHI, entities are required to use encryption where it is reasonable and appropriate for them to do so. In cases where it is not, they must document why it is not and implement an appropriate equivalent. With the increasing availability of affordable encryption software, it is easier today, and thus more reasonable, for covered entities and business associates to encrypt the data on laptops and other portable devices.

Additionally, we believe that the Breach Notification obligations provide an incentive for covered entities and business associates to encrypt where it is possible to do so, given the very public and costly consequences of failing to do so. Many covered entities and business associates report that they are implementing encryption technologies to avoid further breaches. Thus, we expect the use of encryption to continue to grow as a result of these compliance obligations.

EB: During late summer and early fall, we witnessed a "pause" in OCR announcing any settlements with covered entities as Leon Rodriguez left and you joined OCR. Is this evidence of a "kinder, gentler" OCR for the future?

JS: OCR's strong enforcement of the HIPAA Rules is—and has been—very much on track. For example, in December 2014, we announced a resolution agreement with Anchorage Community Mental Health Services (ACMHS) to resolve potential violations of the HIPAA Security Rule, which included payment of $150,000 and requirements that ACMHS adopt a corrective action plan for deficiencies in its HIPAA compliance program and report on its compliance to OCR for a two-year period. Keep in mind, though, that while our settlements involve high-impact cases that send strong enforcement messages to the industry about compliance, they represent a very small fraction of the complaints and compliance reviews through which OCR investigates compliance with the HIPAA Rules. Many of our compliance and enforcement results are achieved by obtaining corrective action and/or providing technical assistance through more informal means, which allows cases to be resolved and compliance issues to be addressed effectively more quickly. Since 2003, our enforcement teams have resolved over 30,000 cases in this way.

OCR's strong enforcement of the HIPAA Rules is—and has been—very much on track.

EB: Many covered entities and business associates struggle with improper behavior by employees who need access to PHI to do their jobs, but then misuse this information. Examples range from employees inappropriately accessing a neighbor or celebrity's medical record, to theft of individuals' information to commit identity theft or tax fraud. Do you see your agency playing a role in helping to stem these types of misuse of PHI?

JS: Absolutely. In resolving cases of employee misuse of PHI, we may require the entities to take any number of actions, based on the facts and circumstances of the case, to prevent similar incidents in the future and to mitigate any consequences to the affected individuals. This may include ensuring that entities appropriately apply their sanctions policies to the employee who committed the offense (which may include dismissal of the employee), reevaluating the risks to the information and improving or strengthening safeguards as appropriate, retraining of employees, revising policies and procedures, and coordination with local law enforcement or other agencies. And in some cases of inappropriate use of PHI, we have achieved and publicized high-profile settlements. We also refer cases to the Department of Justice for criminal enforcement when appropriate. And of course, both the breach reporting obligations under the Rules and our publication on the OCR website of large breaches provide strong incentive for covered entities and business associates to curb employee misuse of PHI.

EB: The HITECH Act clarified that criminal enforcement could be levied against a person—including an employee or other individual—who works for a covered entity and violates HIPAA, even after being adequately trained by their organization. Do you anticipate that OCR will refer more cases to the Department of Justice for criminal prosecution under HIPAA in the future because of this?

JS: We continue to work very closely with the Department of Justice to ensure they have adequate opportunity to pursue appropriate cases for criminal prosecution under HIPAA. Since 2003, OCR has made over 540 referrals to DOJ.

EB: Many privacy officers have compliance backgrounds and have been indoctrinated into ensuring compliance with the Office of Inspector General's (OIG's) seven elements of an effective compliance program, which function as a type of "safe harbor" for well-meaning organizations that have excellent compliance programs, but experience unplanned/unexpected events. Do you see your administration ever supporting adoption of a similar foundation for HIPAA compliance, where well-meaning organizations could achieve "safe harbor" status if their HIPAA compliance programs met certain parameters?

JS: We appreciate that the OIG has been able to create various compliance opportunities for entities under its fraud and abuse enforcement authorities. As OCR's compliance and enforcement program grows, we continue to look for effective opportunities to work with covered entities and business associates to help them ingrain a compliance culture in their organizations.

EB: This interview would not be complete if we didn't ask you a question about the next round of HIPAA audits, mandated under HITECH in 2009. Do you have any specific timeframes or objectives (e.g., educational vs. enforcement-focused) for the next round of audits that you would like to unveil for us here today?

JS: OCR is committed to implementing an effective audit program, and audits are an important compliance tool. They can enable OCR to identify best practices and uncover risks and vulnerabilities not identified through other enforcement tools, provide a proactive and systematic means to assess and improve industry compliance, enhance industry awareness of compliance obligations, enable OCR to target its outreach and technical assistance to identified problems, and offer tools to the industry for self-evaluation and prevention. Organizations should continue to monitor the OCR website for future announcements on the program.

EB: What do you see as your biggest challenge for your administration as we move into 2015?

JS: The movement towards interoperable electronic health records (EHR) is creating new challenges and new opportunities with respect to protecting the privacy and security of health information. HHS is very committed to ensuring appropriate privacy and security protections as it works toward the President's goal of widespread interoperable EHR. Ultimately, as we effectively coordinate health IT activities, we will create an environment in which the health status of the American public is improved while information remains private and secure.

EB: What do you think will be some of the biggest challenges to protecting individuals' PHI five years from now, as the U.S. healthcare system becomes an almost completely digital system?

JS: I think there will be a number of challenges—addressing the privacy and security risks to individuals' health information as "big data" uses become more prevalent, ensuring effective privacy and security, educating and involving patients and consumers in the dialogue about the importance of privacy and security in new health care settings and delivery models, and appropriately addressing the risks to patient information inherent in the use of mobile devices and applications. But it is not inconsistent to protect privacy and security while simultaneously supporting new technologies that improve the delivery of healthcare and health outcomes. We just need to ensure that appropriate protections are in place to safeguard individuals' information as we take advantage of the great opportunities that these emerging technologies present.

EB: Thank you for spending time with us today.

Verisys®

Transparency is Power

Debarred, Excluded, Disciplined, Sanctioned

Can you spot them? Verisys Can!

EQUIP YOUR COMPLIANCE, LEGAL AND FINANCIAL OFFICERS, INVESTIGATORS, HUMAN RESOURCE PROFESSIONALS, CREDENTIALING AND MEDICAL STAFF SERVICES PROFESSIONALS, AUDITORS, PURCHASING AGENTS AND PROCUREMENT TEAMS WITH THE BEST TOOLS IN THE INDUSTRY!

FACIS®

Fraud Abuse Control Information System

Leverage the powerful FACIS® database to pull current and historical published exclusions, sanctions, debarments and disciplinary actions from Federal and State primary source authorities across all jurisdictions and provider types.

FACIS includes OIG, SAM, FDA, DEA, ORI, PHS, state Medicaid exclusions, state contractor and procurement debarment lists, the HEAT Task Force content as well as state and federal Attorney General releases and notices.

- 2,400+ Aggregated Primary Data Sources
- Current and Historical Provider Data
- Single search, batching and monitoring
- Results provided via Real Time Inquiries, Online, SSH and SFTP and API

CheckMedic®

Changing the face of credentialing

CheckMedic is an online credentialing Software-as-a-Service solution that meets and exceeds standards for primary source verification by the Joint Commission, DNV and HFAP.

- Verisys is a fully certified and accredited CVO by NCQA and URAC
- Drastically reduces credentialing, recruitment and on-boarding costs
- Accelerates new appointments and privileging: what once took months can be done in days
- Delivers professional and executive review committees more relevant provider data
- Exclusive endorsement from the American Hospital Association

URAC

ACCREDITED
CREDENTIALS VERIFICATION
ORGANIZATION

NCQA CERTIFICATION

Verisys is fully certified by NCQA for 10 out of 10 verification services.

Verisys Corporation's Credentials Verification Solutions have the exclusive endorsement of the American Hospital Association.

E-Verify

Verisys is an employer agent of E-Verify

VERISYS.COM

Make the smart choice.
Call Us For a Demo.

888.VERISYS
(888.837.4797)

by Shawn DeGroot, CHC-F, CCEP, CHRC, CHPC

Assess and address risks

Shawn DeGroot *(shawn.degroot@navigant.com) is an Associate Director at Navigant Consulting in Denver.* *bit.ly/in-ShawnDeGroot*

In December 2014, the U.S. Department of Health and Human Services, Office for Civil Rights (OCR) announced a settlement with Anchorage Community Mental Health Services (ACMHS) in Alaska for potential violations of the HIPAA Security Rule.

DeGroot

ACMHS will pay $150,000 and adopt a corrective action plan to correct deficiencies in its HIPAA compliance program. OCR's investigation revealed that ACMHS had adopted sample Security Rule policies and procedures in 2005, but the policies were not followed. The security incident was the direct result of ACMHS failing to identify and address basic risks, such as not regularly updating their IT resources with available patches and running outdated, unsupported software.

A focus of the corrective action plan will be on IT patches and software, but the fundamental compliance issue emphasizes the need to perform risk assessments and to audit policies and procedures for effectiveness. "Successful HIPAA compliance requires a common sense approach to assessing and addressing the risks to ePHI on a regular basis," said OCR Director Jocelyn Samuels. "This includes reviewing systems for unpatched vulnerabilities and unsupported software that can leave patient information susceptible to malware and other risks."

Often auditing elements of a compliance program is thought of as applying internal audit standards. Although auditing standards are applicable in financial reviews, the scope of compliance program audits is more diverse. Auditing adherence to and understanding of policies and procedures for privacy and security, competency with compliance education, and elements of the code of conduct are a few examples to demonstrate an effective program. Particularly, consistent application of policies, procedures, and the code of conduct are crucial to avoid turmoil, controversy, and unwanted public scrutiny. Just ask the players and owners in the National Football League (NFL).

> …consistent application of policies, procedures, and the code of conduct are crucial to avoid turmoil, controversy, and unwanted public scrutiny.

In the coming year, when development or modification of the audit plan is due, include auditing policies and procedures with specific focus on security and privacy procedures, and the tentacles that are associated (e.g. cloud computing, access, images). Recovery Auditors (RAs) have consumed inordinate resources and audit time (and still do), but it would be remiss not to place privacy and security as the predominant focus of the compliance audit plan this year.

We are all aware that OCR audits are underway to validate compliance to the HIPAA Privacy and Security Standards. The magnitude of the fine is not always what matters most. Reacting to an incident involves correcting issues after the fact and investing time and resources in managing the post-event media aftermath and public scrutiny. It is a choice to proactively invest in effective auditing by adding privacy and security as a primary focus to the compliance audit plan.

When is a **pause** not really a **pause?**

Named Best in KLAS for RAC Management in 2012 and 2013

Proactively manage all your claims-based audits with

ComplyTrack Claims Audits

While the CMS RAC program is on temporary hiatus, the other auditors are not. And with $5.7B already collected from providers and the funding for the ACA on the line, you can be sure the RAC program will return with a vengeance. **ComplyTrack Claims Audits**, designed to put you in control of the complete claims audit life cycle, provides the flexibility to manage not only requests from RACs, but also from MACs, MICs, ZPICs, and commercial payer audits. Take advantage of this time—get the solution you need to stay ahead of all the auditors and protect your bottom line.

complytrack.com

Wolters Kluwer

by Mia Okinaga

Fraud control strategy: Where to focus limited resources

» Focusing on the right initiatives will advance your fraud control program.
» Identifying anomalies and outliers will help create meaningful information for leadership.
» Enhancing data analytics tools allows for an organization to stay in front of regulators.
» Increasing the velocity of integrated learnings will create a stronger and leaner organization.
» Establishing an integrated staged fraud-control program will yield returns on investments.

Mia Okinaga *(mia.s.okinaga@kp.org) is Vice President of Reimbursement Compliance, Fraud Control, and Compliance Information and Analytics for the National Compliance, Ethics & Integrity Office of Kaiser Permanente in Oakland, CA.*
bit.ly/in-MiaOkinaga

"Health care fraud is a rising threat, with national health care spending topping $2.7 trillion… rooting out fraud in health care is one of the Federal Bureau of Investigation's top criminal priorities," according to the Centers for Medicare & Medicaid Services (CMS).[1] Most organizations battling fraud, waste, and abuse are usually in need of more resources, not less, and coming up with these resources can be a challenge. Returns on investments can be positive, but even then, most organizations want "lean and mean" fraud control programs. When resources are limited, having a strategy based on the state of the program will provide guidance on where to focus restricted resources to maximize return.


Okinaga

As compliance professionals, how do we best protect our organizations from committing and/or being victimized by fraud? With limited resources, it can be overwhelming. Health plans are expected to use data in their fraud prevention programs, and CMS is deploying data analyses in their audits to detect things such as excluded providers, duplicate billing and services, and anomalies (e.g., upcoding and non-medically necessary procedures). This article provides an overall framework and recommendations on where to focus those resources, depending on the maturity of the fraud control program.

Fraud control programs generally have three stages that are based on the current developments in any given organization. Table 1 is a simple chart to define each of the three stages in the continuum.

Reactive	Proactive	Integrated
▶ Denial of seriousness	▶ Defined controls and processes	▶ Aligned operational goals and joint initiatives
▶ Ad hoc	▶ Proactive detection	▶ Investigations with law enforcement and peer organizations
▶ Dependent on heroics	▶ Timely response to allegations of misconduct	▶ Collaboration among subject-matter experts for dynamic integration
▶ Not perceived as a necessary cost	▶ Perceived as a necessary cost	▶ Positive return on investment ▶ Perceived as a necessary cost

Table 1: Types of fraud control programs

Reactive fraud control program

A reactive fraud control program is one where an organization's leadership is not aware of its vulnerabilities to fraud, and the program is not perceived as a necessary cost. It is usually smaller companies that encounter fewer incidences of fraud that may incur higher costs-per-incident as the trade-off for not sustaining an ongoing program. In this stage, surprises are likely, so leadership should have a high risk tolerance. With little to no structure or strategy in place, fraud cases are often handled haphazardly. In order to prove the wrongdoing, heroics are required to gather the evidence, convince leadership, and successfully refer to law enforcement for criminal prosecution.

What to focus on

The most important thing to do in this stage is to make the case with leadership to implement a fraud control program. Define the threat and ask management how comfortable they are with their risk mitigation strategies. To define the threat, obtain the most recent and relevant activity from the Department of Justice, Office of Inspector General, State Attorney General, and the National Healthcare Antifraud Association, among others. For instance, the Department of Justice and Federal Bureau of Investigation annually publish the number of criminal healthcare fraud investigations and convictions. Consider the threats that most apply to your organization. Medicare Advantage Organizations can reference Chapters 9 and 21 of 42 CFR, which outlines fraud control program requirements.

Many regulatory agencies and insurers are expecting evidence of a robust fraud, waste, and abuse program where reports of losses, numbers of cases, and referrals to law enforcement are required. Sharing these requirements with your organization's leadership will likely lead to a dialogue about the kind of fraud control program leadership wants and expects.

Proactive fraud control program

A majority of companies' fraud control programs fall into this stage. A proactive fraud control program is one where an organization's leadership perceives the program as a necessary cost. Typically, an organization employs a skilled, special investigations unit with backgrounds in state and federal law enforcement and experience in white-collar crime. A fraud or employee hotline and case management system is generally used and regularly monitored. The organization's timely response to allegations of misconduct can be demonstrated by a compliance officer. Risk assessments in the form of interviews and surveys are completed, reviewed, and acted upon. Processes are defined and controls are in place to report fraud, waste, and abuse; conduct investigations; and implement corrective action plans. Having a program establishes credibility and trustworthiness in the event of an audit by regulators or law enforcement; organizational leadership is demonstrating evidence that any misdeeds were unintentional.

What to focus on

In the proactive stage, organizations should focus on enhancing their data analytics tools. Doing so allows for an organization to stay in front of regulators and proactively identify risks. Meet with leadership to understand the system edits and fraud controls that are currently in place. Partner with other risk management units, such as Internal Audit and the Controller's Office, to identify anomalies and outliers that should be further reviewed. Hone in on claims, accounts payable, payroll, pharmaceuticals, and durable medical equipment utilization, as these are inherently high-risk areas for fraud, waste, and abuse. A few examples of data analytics to keep in mind are:

- **Claim payments** – High dollar, foreign claims, global surgical charges unbundled, excluded providers, short lengths of stay, coordination

of benefits, Medicare secondary payer, services after death, basic vs. advanced ambulance services, and radical height-and-weight changes.

- **Accounts Payable** – Duplicates in billing and services; employee and vendor addresses, telephone numbers, and names; spike billings; and unexpected and/or expedited payment trends.
- **Payroll** – Payments after termination and transfers, duplicates, frequency of manual checks, and changes in direct deposits and other debits.
- **Pharmaceuticals** – Clinically administered drug utilization, drug seeking behavior for opioids, life enhancement drugs (e.g., Viagra), items easily resold (e.g., glucose test strips), early refills, unusual indirect and direct remuneration trends, and drugs dispensed without a recent provider visit.
- **Durable medical equipment** – Use of ambulatory continuous positive airway pressure (CPAP) and oxygen, use of beds, rental payments beyond expiration, and payments without a recent provider encounter.

Integrated fraud control program

Integration is the leap to a higher plane in terms of partnerships with regulators, law enforcement, and peer organizations. At this stage, fraud control programs may present a positive return on investment in the form of recoveries, avoidances, and enhanced work flows. Senior and functional leaders demonstrate high levels of awareness when it comes to fraud risks specific to their areas. Dedicated multi-functional work groups or committees meet periodically to address proactive detection of anomalies. This includes sponsorship of analytical data studies; review and investigation of the anomalies and trends; oversights of changes in procurement, contracting, payment, and utilization management; and assessments of other work flows that strengthen the organization. Leaders of inherently high fraud-risk areas have shared goals with the compliance program. Fraud-control program personnel collaborate with law enforcement, peer companies, and industry organizations to combat fraud in the form of joint analyses and investigations.

What to focus on

The most important thing to do is increase the velocity of integrating learnings from the fraud, waste, and abuse cases into the organization. The faster change is implemented, the stronger and leaner the organization becomes. In order to increase velocity of change, there has to be strong working relationships and high levels of trust and collaboration among stakeholders. As organizations move into the integrated stages of a fraud control program, they will begin to see an increase in returns on investments in the form of savings from recoveries (e.g., credit memos and checks), avoidances (e.g., overpayments prevented), and restitution from criminal activity. A periodic report presenting numbers associated with these savings can demonstrate to leadership the value of a robust fraud control program.

Focusing on the right initiatives can advance your fraud control program. Fraud control programs that are in the initial reactive stages should focus on making the case for a compliance program with risk mitigation tactics emphasizing high-profile internal cases and what law enforcement and anti-fraud taskforces are targeting. This will provide leadership with direction, support, and focus. More established proactive programs should focus on sharpening data analytics tools and partnering with other risk management units to proactively detect fraud, waste, and abuse. Advanced integrated programs should focus on increasing the velocity of integrating learnings into the organization to maximize the return on the organization's investment in the fraud control program.

1. Centers for Medicare & Medicaid Services: *CMS Medicare Advantage and Part D Fraud Handbook*, March 2014. Available at http://bit.ly/1Cxuhrc

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

2015 Basic Compliance Academies

from the Health Care Compliance Association

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

SOLD OUT:
March 9–12 • Las Vegas, NV

LIMITED SEATS REMAIN:
April 27–30 • Orlando, FL

June 8–11 • Scottsdale, AZ

August 10–13 • New York, NY

September 14–17 • Chicago, IL

JUST ADDED:
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

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

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

by Nadia Fahim-Koster, CISSP, HCISPP

Is your privacy monitoring up to snuff?

» Understand the requirements that drive the need for continuous logging and monitoring.
» Recognize the implications of the HIPAA Breach Notification Rule.
» Proactively position your organization to monitor risks of data breaches.
» Develop a monitoring program that is scalable to your organization.
» Learn how to develop a clear and accountable communication plan.

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

More than ever, healthcare organizations are at a greater risk of falling short on patient privacy requirements. Since the Health Insurance Portability and Accountability Act (HIPAA) was passed in 1996, the healthcare industry has seen a steady stream of regulations, such as the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and the HIPAA Breach Notification Rule of 2013. The HITECH Act, among other things, provides incentives for healthcare providers to make the transition from paper to electronic health records (EHR) systems and create opportunities for jobs related to the "meaningful use" of healthcare IT. The HITECH Act also has strengthened HIPAA fines and penalties for privacy violations.


Fahim-Koster

In order to mitigate risks to the inappropriate disclosure of patient protected health information (PHI), HIPAA/HITECH requirements, such as those listed below, drive the need for continuous logging and monitoring:

- The HIPAA Privacy Rule minimum necessary standard "requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information."[1] It should be noted that this has been a top priority target area for federal enforcement by the Office for Civil Rights (OCR).
- The HIPAA Security Regulation calls for organizations to implement procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports,[2] and to implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use ePHI.[3]
- 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.

So what does this all mean to you? It means that you should implement a comprehensive privacy monitoring program that will position your organization to not only proactively identify when there is risk of a data breach, but also align you with HIPAA/HITECH

auditing requirements. Monitoring refers to both application-level access to PHI as well as any supporting infrastructure, such as servers, workstations, network devices, etc.

By following the seven steps outlined below, you should be well on your way to establishing a robust monitoring program that is scalable to the size and complexity of your organization and systems.

1. Define roles and responsibilities

The first step in your program is establishing who in your organization will be responsible for different aspects of the program. Some of the questions you should be asking and answering are:

A. Who will own the process?

It is highly recommended, based on industry best practices, for the privacy or security officer of the organization to own the process, sometimes with collaboration between both roles. This is particularly important if the program will rely on tools that can provide you with the capabilities to examine logs that will satisfy both privacy and security requirements. Application analysts, as well as the IT department, should also be involved to handle some of the technical details that will be required to pull data out of your electronic health records.

B. What roles within your organization should be involved in the program?

Your Human Resources (HR) department should be included in the program, because you are sure to need them when your findings point to potential policy violations on the part of your employees.

Lastly, don't forget to bring your legal counsel on board—as well as your Public Relations and Communications department—should you find yourself in a data breach situation that would require your organization to notify not only the patients affected by the breach, but potentially the media as well as Health and Human Services.

2. Establish monitoring policies and procedures

Once your roles and responsibilities are defined, your next step should be to develop policies and procedures that take into consideration the following criteria/factors:

A. The type of monitoring you will be performing

This could be either continuous or on a sample audit basis. Continuous monitoring will give you the ability to detect inappropriate access and minimum necessary access violations. It will help you to investigate these incidents and let you assess whether you have experienced a breach. In addition, proactive monitoring, when well-communicated within your organization, often acts as a powerful deterrent with employees. Sample audit basis monitoring is what most organizations default to when they are unable to conduct proactive monitoring due to a lack of resources, both human and capital. This type of monitoring relies on selecting a random sample logs to review on a periodic basis. In both continuous and audit sampling monitoring scenarios, your policies and procedures need to specify how often you will audit, who will perform the audits, what the procedure is to handle incidents, investigations, resolutions, breach notifications (if applicable), and sanctions.

B. What to monitor

Your policies need to describe up front what behaviors your organization will be monitoring. For instance, will you be monitoring inappropriate access to patient records based on VIP, neighbor, or family snooping? What about access to very sensitive information, such as mental health records, HIV/AIDS, sexually transmitted diseases, or substance abuse?

Make a list of all potential disclosures that could cause harm to your organization and identify how you want to handle monitoring for such access.

3. Identify your data elements and related sources

Now that you have a good idea of what it is you want to monitor and for what reasons, your next step is to identify what data elements would be necessary to include in your monitoring strategy and where these data elements reside.

For instance, some basic demographic elements needed would be employees' names and ID numbers, patient names, DOBs, any unique identifiers (e.g. Medical Records numbers, Social Security numbers), addresses, and any other information you can use to put together a profile to see which employees accessed information on which patients. In addition to demographic information, you will want to have access to clinical information, such as diagnosis codes, dates of service, medication lists, treating physicians, etc.

All demographic information associated with your employees most likely resides in your HR system. Demographic information associated with your patients could be in the patient registration system or EHR systems.

The clinical information will reside in any clinical information system your organization maintains, which could be one or many.

Once you have a clear picture of which data elements are needed and where to find them, you are ready to define your logging requirements.

4. Define and implement logging requirements

The fourth step in your monitoring program is to define your logging requirements. You will have to determine if the clinical, financial, and HR systems have auditing capabilities, and if they do, whether the audit logs are enabled. Legacy applications may not have logging capabilities, which would make it virtually impossible for you to include them in your monitoring program. However, for all applications and systems that are capable of creating audit logs, you will need to work with your IT department and applications team to ensure that the logs are enabled and identify how often the logs are collected, how long they will be kept, and in what format they will be generated.

In particular, decisions around log storage size need to be considered, because some applications can generate very large log files that can take up your storage space very quickly.

In particular, decisions around log storage size need to be considered, because some applications can generate very large log files that can take up your storage space very quickly. Determine how many days or months of live logs you will keep in place (e.g., any ongoing investigations or pending investigations should have audit logs handy), and how long you will archive the logs once they are moved off the live schedule.

Determine also the format of the reports you will be reviewing. Some EHR systems have native audit tools. These tools can provide you with a very good picture, but they may not always provide you with reports that are easy to read and interpret. As a result, these reports may require further manipulation from your in-house or contracted report writers to be able to run queries to provide

you with the specific reports you need, such as "break-the-glass" reports or who accessed VIP and confidential patient files.

Lastly, these native tools may not easily integrate with other vendor systems (such as your HR system or financial systems) if they are separate from your EHR system. You will then need to create queries or reports that cross over the various systems or you may need to purchase a third-party tool that will provide you with the ability to correlate data from disparate systems.

5. Define resources requirements

You have now worked through the first four steps in your program and should have a pretty clear idea on the level of complexity and scope of your monitoring program. You are now ready to define your resources requirements, both human and technical.

In other words, based on what you've identified so far, you need to identify whether a third-party tool is needed. If the decision is to acquire one, you need to take into consideration that you might need a resource to run the tool. You will once again have to work with your IT department to identify a resource for them that will implement the tool and help run it.

If you determine that you will not use a third-party tool, but will instead rely on disparate logs from different systems and will work with access databases to correlate your logs (which is a highly resource intensive process), you have to ask yourself whether you have the resources in place to handle the new workload.

In other words, based on what you've identified so far, you need to identify whether a third-party tool is needed.

Keep in mind that at this point in your program establishment, you might realize that you do not have the required resources it would take to implement a fully functional monitoring program, and you may have to go back through your steps and adjust accordingly. For instance, you might find that to start with, you will investigate events or incidents as they are brought to your attention, and perhaps run two or three reports a month on a proactive basis. Once you start your program and start getting buy-in from your management team, you may be able to scale up and expand the program to a full-fledged monitoring program.

6. Incident response handling

Once your monitoring program is in place, you will start dealing with incidents that you will have to investigate in order to determine your course of action. Some incidents will result in breaches, others might be false alerts or misconduct from an employee without rising to the level of a breach. Note that it is during this step that you will need to outline the HITECH Breach Notification requirements in your Incident Response plan. There is a four-step breach analysis that needs to be performed in order for you to establish whether an incident rises to the level of a breach notification event.[4]

Your processes will need to include incident response handling so that you know exactly which course of action to take depending on the outcome of your investigation. You will need to identify who to notify in case

of a breach (e.g. your Legal department, your Risk Management department, your PR and Communication department, your HR department, etc.) and what steps to follow as you are progressing through your investigation.

7. Communication plan

At this point in your program development, you are ready to start thinking through the last step, which is your communication plan to the organization. Every workforce member must have a clear understanding that their actions are being monitored and what the consequences are in case of a policy violation. The communication plan should make it clear that anyone using your organization's electronic records is subject to the monitoring program and will be held accountable for their actions.

Last, but not least, the plan should identify the monitoring program start date so that there are no questions in anyone's mind that, moving forward, all of their actions will be recorded and monitored.

Conclusion

Developing and implementing a robust privacy monitoring program can be a daunting task. However, by following the seven steps outlined in this article, you will implement a program that is scalable to the size of your organization and available resources. Once this program is in place, you need to make sure to set up a process in place to review and update your program periodically (i.e., annually, bi-annually, or as the regulations change), to keep up with emerging technologies and requirements.

1. U.S. Department of Health and Human Services; "*Health Information Privacy: Minimum Necessary Requirement;*" OCR HIPAA Privacy; December 3, 2002, revised April 4, 2003. Available at http://1.usa.gov/13u6JqK
2. 45 CFR Part 164.308 (a)(ii)(D)
3. 45 CFR Part 164.312 (b)
4. 45 CFR 164.402

Join your peers at the primary networking and educational event for compliance professionals working in research compliance

Register by April 8
SAVE $250

Research Compliance Conference

May 31–June 3, 2015 | Austin, TX

hcca-info.org/research

QUESTIONS? katie.burk@corporatecompliance.org

TWO CONFERENCES FOR THE PRICE OF ONE

Complimentary access to SCCE's Higher Education Compliance Conference is included with your registration. Build your own schedule and attend sessions at both conferences!

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

by David Hoffman, JD, FCPP

Using compliance principles to address hand hygiene

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

As I write this, the country is bracing for flu season to begin in earnest. The CDC has made its recomendations and hopefully, those patients at risk will take heed and get a flu shot. I often wonder why healthcare-associated infections (HAIs) are so troublesome to remedy, and why routine hand-washing is so difficult to enforce. If we can't get healthcare workers to wash their hands, how do we expect them to act compliantly with all of the other complex clinical and regulatory requirements? As a compliance officer routinely asks, "What are the barriers to compliance?"

Hoffman

The World Health Organization (WHO) noted:

> Healthcare-associated infections usually occur when germs are transferred by health-care providers' hands touching the patient. Of every 100 hospitalized patients, at least 7 in high-income and 10 in low-/middle-income countries will acquire a healthcare-associated infection. Among critically ill and vulnerable patients in intensive care units, that figure rises to around 30 per 100. Every year, hundreds of millions of patients around the world are affected by healthcare-associated infections, a high proportion of which is caused by germs that are resistant to antimicrobial drugs.[1]

The WHO has published several invaluable tools on this issue, including a Hand Hygiene Self-Assessment Framework 2010.[2] Additionally, the Pennsylvania Patient Safety Authority recently issued an Advisory[3] which focused on hand hygiene compliance in Pennsylvania and provided meaningful interventions.

What can a compliance officer do to facilitate compliance with routine hand-washing? Obviously, this is a "culture" issue, and we have seen how difficult it is to create a culture of compliance, but we know that compliance occurs with effective training and education followed by enforcement for non-compliance. Additionally, we can implement an audit and monitoring program that includes direct observation of staff (by colleagues, camera) and other uses of technology, including electronic monitoring. I was recently told of a nursing home that has used technology to track and prove that staff was, in fact, actually going into residents' rooms. Why not add a monitoring of hand hygiene to that existing monitoring process?

Finally, we know that there is a behavioral component to getting this right. Staff must be educated as to why compliance with hand hygiene is so important. Reckless conduct related to hand hygiene must be responded to as part of an effective compliance program. Disregard for hand hygiene interventions should be actionable under an organization's effective compliance program.

1. World Health Organization: Clean Care is Safer Care: The evidence for clean hands. Available at http://bit.ly/1zjFyOy
2. World Health Organization: Patient Safety: Hand Hygiene Self-Assessment Framework 2010. Available at http://bit.ly/1xtVB5q
3. Pennsylvania Patient Safety Advisory: A Systems and Behavioral Approach to Improve Hand Hygiene Practice. December 2014. Available at http://bit.ly/1yhmlx2

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Research *Basic Compliance* Academies

San Diego, CA
March 2–5, 2015

Orlando, FL
November 2–5, 2015

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

SOLD OUT **San Diego, CA**
March 2–5, 2015

Las Vegas, NV
June 15–18, 2015

Orlando, FL
November 2–5, 2015

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:
jennie.nguyen@corporatecompliance.org

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

REGISTER EARLY
ACADEMIES FILL FAST

by Peter A. Khoury, MHA, MJ, CHC

Compliance challenges in new chronic care management code

» A new per-beneficiary-per-month chronic care management code will be available in 2015.
» The new code recognizes non–face-to-face services for patients who have chronic conditions.
» Evaluate clinical, technological, and compliance infrastructures before billing.
» Demonstrate and document the effectiveness of training about the code by conducting pre-session and post-session assessments.
» Conduct regular reviews early-on, and implement controls to monitor use.

Peter A. Khoury *(pkhoury@deloitte.com) is a consultant in the Philadelphia office of Deloitte & Touche LLP.* /in/khourypeter

Since January 1, 2015, the Centers for Medicare & Medicaid Services (CMS) has started to reimburse providers for chronic care management (CCM) services on a per-beneficiary-per-month basis. This service provides a new source of revenue for organizations with large patient populations that have at least two chronic conditions. This is part of the federal government's emphasis on decreasing both the cost of medical care and readmissions by enhancing primary care efforts for beneficiaries. The code opens the door to financial reimbursement for previously non-reimbursed services, but it brings with it a number of compliance risks and challenges for healthcare organizations.

Khoury

In 2013, CMS finalized their Medicare Physician Fee Schedule (MPFS) for 2014, which described a new CCM code, GXXX1. This Healthcare Common Procedure Coding System (HCPCS) code, which was converted in 2014 to Current Procedural Terminology (CPT) code 99490, reimburses providers and qualified healthcare professionals for the coordination of CCM services. This new per-beneficiary-per-month code, if reported accurately and managed correctly, can create a new monthly source of revenue for providers for non–face-to-face services provided to these patients. As outlined in the 2015 MPFS final rule, code 99490 will correspond to 20 minutes of service during a calendar month furnished to patients with two or more chronic conditions that are expected to last at least 12 months or until death and that place the patient at significant risk of death, acute exacerbation, or functional decline.[1]

To avoid duplication of services, practitioners may not bill for transitional care management (99495-6), home healthcare supervision (G0181), hospice supervision (G0182), or end-stage renal disease (90951-70) services during the same reporting period. Only one practitioner can furnish and bill for CCM services for a beneficiary during a calendar month, and the services can be initiated through annual wellness visits, initial preventative physical examinations, or evaluation and management visits.[2]

The 2015 MPFS final rule, released on November 13, 2014, provides further guidance on this new code. Even with this guidance, care providers and compliance professionals must be aware of the complex requirements that must be satisfied to bill for these services and establish controls that minimize exposure to compliance risks, such as billing for services not rendered.

2015 proposed rule changes to GXXX1

The 2015 MPFS proposed rule outlined changes to code GXXX1, which was finalized in 2014. The 2015 proposed rule suggested three major changes. In the 2014 final rule, an exception was created for "incident to" supervision requirements outside of normal business hours. The 2014 final rule outlined that clinical staff were able to provide CCM services if under general supervision of a provider and if the clinical staff member was a direct employee of the practice or provider handling the service.[3]

The first suggested change in the 2015 proposed rule sought to remove the requirement that clinical staff must be direct employees.[4] The second proposed change in the 2015 rule was to permit any time spent by clinical staff on CCM services to be counted toward the 20 minute minimum, provided that all requirements for billing for the service were met and that the clinical staff member was under the general supervision of a provider.[5]

The third proposed change was that CCM services provided must be documented through an electronic health record (EHR) that is accessible to all members of the care team, even outside of regular business hours, inside or outside of the practice. The system, as proposed in the 2015 rule, must also be certified by a body authorized by the National Coordinator for Health Information Technology.[6]

There are a number of elements required to bill for these services as established in the 2014 MPFS final rule,[3] which include:

- Beneficiary notification of CCM service availability,
- Obtaining written agreement for the beneficiary to have patient information shared with other members of the care team,
- Documenting the explanation of CCM services, including a beneficiary's decision to participate or not participate in the program,
- Providing a written or electronic copy of the care plan to the beneficiary with documentation in the EHR that the plan was given to the beneficiary,
- Providing the beneficiary with an explanation that participation in the program is voluntary and can be terminated at any time, and finally
- Only one practitioner can furnish and receive reimbursement for CCM during the service period.

CMS continued to make way for the availability of the new HCPCS code in 2015, but some uncertainty existed around its final form. In 2013, the American Psychiatric Association's summary of the 2014 MPFS final rule stated that a group of specialty associations were working with a CPT Workgroup to create a CPT code to replace the HCPCS code.[7] Rule makers have listened closely to specialty association feedback in the past, and it looks like they have listened to commenters again, amending both their previously finalized 2014 rule and the 2015 proposed rule.

CMS adopts 2015 final rule and proposes additional changes

The 2015 final rule with comment period provides further guidance on CCM services. First, after considering comments from stakeholders, the rule changes the original GXXX1 HCPCS code to CPT code 99490, while also changing the service period from 30 days to a calendar month.[1] The final rule recognizes the challenges patients may face accessing timely CCM services if clinical staff providing the CCM services, even during off hours, must be direct employees of the supervising practitioner's office. Therefore, the 2015 final rule amends the prior 2014 rule, removing the requirement that clinicians providing CCM services must be a direct employee of the supervising practitioner's office. The 2015 final rule also allows clinical staff, under general supervision of a practitioner, to count time providing

CCM services towards the time requirement for billing the service every month as long as the rest of the "incident to" requirements are met.[8] Many times, these services are non-face-to-face encounters and may occur when the supervising provider is not physically present.

The 2015 final rule also codifies a new scope of service element that requires CCM to be provided through a certified electronic health record (EHR) for many services provided, such as developing the care plan through problem list updates and communicating with recipients of CCM services through non–face-to-face methods. The final rule also modifies the 2015 proposal and creates a requirement that the electronic record must be certified using the prior year's EHR Incentive Programs criteria.[9]

Compliance challenges exist

It is important for compliance professionals to evaluate the elements of the required scope of services to bill for the new CCM code and determine how their current infrastructure meets the demand of such requirements. Where current clinical, technological, or control infrastructures do not meet the demand of the billing requirements, the compliance team should work collaboratively with important stakeholders to provide essential input on building these measures prior to billing for these services. The following are three important areas of emphasis that compliance professionals, clinical leadership, and management should pay particular attention to, because they are critical components of billing for CCM services.

Patient eligibility

CCM services were created to assist patients with specific risk factors. Therefore, appropriate levels of documentation should be found in the beneficiary's medical record that outline the number of chronic conditions present, the extent of the chronic conditions, and the impact these chronic conditions will have on their health and well-being in the future. Furthermore, the beneficiary's written consent to participate in the voluntary CCM program should also be documented in the record.

Provider eligibility

The 2015 final rule amends the 2014 final rule, allowing clinical staff to count time spent on CCM services towards the monthly 20 minute minimum requirement as long as they are under the general supervision of a practitioner and all other "incident to" requirements are met.

Service eligibility

Proactive steps should be taken to confirm that practitioners billing for CCM services are not also billing for overlapping codes. A number of other service elements are required to be met before a practitioner can bill for CCM. These are outlined in the 2015 final rule, including 24/7 access to and successive appointments with a dedicated member of the care team. The new service requirements outlined in the 2015 final rule related to EHRs are important to discuss, particularly that the EHR will now be a central component through which CCM services will be documented. The beneficiary's care plan must be accessible to all practitioners, both within and outside of the practice, during and outside of normal business hours. This does not stipulate that those involved in providing CCM services outside of normal business hours must have access to the full medical record, as outlined in the 2014 proposed rule, but it does pose a compliance risk for practices that do not have EHR system compatibility, and it brings user access control risks into question.[9]

Training

Overall, specific training and education for providers and their clinical staff who perform elements of CCM services can bring forward in a clear fashion the billing requirements for this new code. Compliance professionals can demonstrate the impact of the training and

education sessions by comparing pre-session and post-session assessment results.

Compliance professionals working with clinical leadership should also thoroughly review what services clinical staff can provide, document, and bill for under the general supervision of a provider. The compliance staff in collaboration with the Coding and Billing departments should also conduct periodic reviews for supporting documentation and appropriate code selection for providers and practices that use these codes. Finally, as healthcare entities more broadly develop care coordination strategies for their patients, a comprehensive review of the current technological infrastructure should occur to determine compliance risk areas that result from the changing regulatory environment, and strategies should be developed to anticipate and reduce these risks in the future.

Final thoughts

CCM provides financial reimbursement for delivering important services to patients and improving transitions across the care continuum with novel delivery mechanisms. Healthcare entities must be cognizant of specific compliance risks they may encounter while providing these services and develop solutions in consultation with counsel and important stakeholders to mitigate these challenges. Compliance professionals who are employed by healthcare entities that are instituting care coordination programs must closely follow the development of these new codes and ask important questions to determine patient, provider, and service eligibility for CCM services. It is good practice for compliance professionals to stay well-informed of the changes proposed and finalized by CMS through the MPFS and consider becoming engaged in the comment period as stakeholders in the process of shaping new rules.

This article contains general information only and Deloitte is not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this article.

1. 2015 MPFS final rule, 79 FR 67716 at 1 – 67719, published November 13, 2014.
2. 2014 MPFS final rule, 78 FR 74421 at 4 –74427, published December 10, 2013.
3. 2014 MPFS final rule, 78 FR 74414 at K – 74427, published December 10, 2013.
4. 2015 MPFS proposed rule, 79 FR 40365 at 2 – 40367, published July 11, 2014.
5. 2015 MPFS proposed rule, 79 FR 40366, published July 11, 2014.
6. 2015 MPFS proposed rule, 79 FR 40367 at 3 – 40368, published July 11, 2014.
7. American Psychiatric Association Summary of Final Rule for the 2014 MPFS.
8. 2015 MPFS final rule, 79 FR 67719 at 2 – 67721, published November 13, 2014.
9. 2015 MPFS final rule, 79 FR 67721 at 3 – 67729, published November 13, 2014.

by Susan Prior, CHC and Cristine Vogel, MPH

340B drug program: Hospital audit readiness

» Develop a comprehensive oversight and monitoring strategy to remain compliant within the complexities of the 340B program.
» Define clear policies and procedures for patient and prescriber eligibility.
» Review eligibility requirements and regularly update HRSA database.
» Incorporate frequent self-audits and annual external audit to ensure readiness.
» Develop community benefit plan to ensure HRSA's program intent.

Susan Prior *(sprior@vantagepointconsult.com) is the President and COO and* ***Cristine Vogel*** *(cvogel@vantagepointconsult.com) is a Senior Consultant for VantagePoint HealthCare Advisors in Hamden, CT.*

The 340B drug pricing program is designed to help certain safety net healthcare providers extend services to the underserved and uninsured. It was established under the Veterans Health Care Act of 1992 in section 340B of the Public Health Service Act, and is managed under the federal Health Resources and Services Administration (HRSA).[1] The 340B program enables eligible facilities to purchase outpatient drugs at discounted prices; discounts can be up to 50% of the drug's cost.[2] Eligible facilities, called covered entities, receive discounts from the drug manufacturers and are expected to pass the revenue gains toward services targeted at populations in need or to reduce the cost of patients' prescription drugs.

Today more than 7,800 entities are covered by the program. Federal officials estimate that the 340B program accounts for $6 billion in outpatient drug spending with an estimated savings of $1.6 billion for 340B providers. Some experts say that with the expansion of this program under the Affordable Care Act (ACA), the program spending could possibly double.[3]

In response to the increased number of entities participating in the 340B program, HRSA is increasing the number of audits conducted with covered entities. Although the FY2014 audits are still in process, HRSA reports that as of August 2014, 91 audits of covered entities have been conducted, including 1,347 outpatient facilities and 3,811 contracted pharmacies (entities may have multiple outpatient sites and are able to contract with multiple pharmacies). This far exceeds the number of audits in FY2012, which included 94 audits of covered entities (718 outpatient facilities and 1,937 contracted pharmacies).[4]


Prior


Vogel

Given the complexity of the 340B program, hospital systems that have multiple campus locations, outpatient clinic sites, and contract pharmacies need to develop a comprehensive oversight strategy and compliance monitoring program. Although the probability of an audit may seem low, the stakes are high when failure to comply can result in large repayments to the drug manufacturers or program termination. Audit readiness is critical to the long-term sustainability of the program.

Confirm eligibility requirements

Assessing the hospital's 340B program is essential to ensure policies and procedures

are in place for all federal requirements. Equally important is that the hospital is adhering to its own policies and procedures. Having well-defined procedures, training, and monitoring that address these three key areas are critical:

- Hospital eligibility
- Patient eligibility and diversion prohibition
- Prescriber eligibility

340B hospital eligibility requirements

There are 17 covered entity categories, including 11 categories that qualify through federal grant programs and six categories for hospitals (see Table 1).

Each category has its own eligibility requirements. For hospital eligibility, they must be designated as a not-for-profit and be one of the six hospital categories listed in Table 1. Secondly, the hospital must meet at least the minimum Disproportionate Share Hospital (DSH) percentage for the specific hospital type as reported on the most recent Medicare Cost Report. The percentage varies with hospital categories (see Table 2).

After a hospital applies and is approved to participate in the 340B program, the hospital must register in the HRSA database. This information includes the hospital's contact information, hospital and clinic location(s),

Federal Grantees/Designees	Certain Hospitals
▶ Federally Qualified Health Center ▶ Federally Qualified Health Center Look-A-Likes ▶ Title X Family Planning Grantees ▶ State AIDs Drug Assistance Programs ▶ Ryan White Care Act Grantees (A,B,C,D,F) ▶ Black Lung Clinics ▶ Hemophilia Treatment Centers ▶ Native Hawaiian Health Centers ▶ Urban Indian Organizations ▶ Sexually Transmitted Disease Grantees ▶ Tuberculosis Grantees	▶ Disproportionate Share Hospitals ▶ Children's Hospitals ▶ Critical Access Hospitals ▶ Free-Standing Cancer Hospitals ▶ Rural Referral Centers ▶ Sole Community Hospitals

Table 1: Categories of 340B Covered Entities

Hospital Category	DSH Percentage
▶ DSH Hospitals ▶ Children's Hospitals ▶ Free-Standing Cancer Hospitals	>11.75%
▶ Rural Referral Centers ▶ Sole Community Hospitals	≥ 8%
▶ Critical Access Hospitals	Not Applicable

Table 2: DSH Percentage by Hospital Category

contracted pharmacies, and Medicaid billing information. Each outpatient clinic site listed in the database needs to appear as a reimbursable clinic on the most recently filed Medicare Cost Report, each site needs to be an integral part of the hospital, and be used by patients that meet the 340B patient definition. If any of this information changes during the year, the hospital must update the HRSA database during one of the designated quarterly periods.

Additionally, annual recertification is required to ensure that the information is not only current for the following year, but also that the 340B hospital continues to meet eligibility requirements. If a covered entity fails to recertify, participation is automatically terminated.

340B patient eligibility requirements

Although eligibility to participate in the 340B program is defined at the covered entity level, not every patient who receives care at the covered entity level can receive drugs purchased through the 340B program. HRSA defines a patient as eligible for 340B when the hospital can demonstrate these three parameters regarding the patient: (1) the patient has an established healthcare relationship with the hospital or services provided by the hospital; (2) the hospital maintains health records of the services provided to the patient; and (3) the patient receives services from a provider who is employed or under contractual or other arrangements with the hospital.

The 340B drug program is applicable for certain outpatient drugs and allows the participating hospital to use the discount. It is the responsibility of the 340B hospital to make sure only patients of that hospital are being prescribed 340B drugs and that the hospital is receiving discounts only for patients of the hospital.

When a physician under contract with a 340B hospital provides care to an eligible patient, but that care is outside of the physician's contractual agreement or provided at a site not designated as a 340B location, the patient is no longer 340B-eligible according to HRSA's definition. The hospital must therefore, have a process to determine and monitor patient eligibility as it relates to the prescriber and location. Additionally, the hospital must ensure that proper data is provided to the pharmacies so the pharmacies are aware when prescriber and patient eligibility changes from 340B status. 340B hospitals must be able to identify not only that the patient at each site of service is eligible, but also that the physician is an eligible 340B prescriber at that site of service.

- **Preventing diversion**

Diversion occurs when 340B drugs are dispensed to ineligible patients, a scenario where it appears as though the hospital is transferring or re-selling 340B-purchased drugs at a non-340B price. The hospital is responsible for verifying the eligibility of its 340B patients and is responsible for providing their pharmacies with the proper data so that only 340B drugs are prescribed and dispensed to eligible 340B patients. Because diversion is prohibited, hospitals must have a plan to conduct regularly scheduled monitoring for compliance. HRSA recommends monthly monitoring.

340B prescriber eligibility requirements

A 340B hospital must demonstrate that a healthcare practitioner is either an employee, under contract, or has some "other arrangement" that satisfies the eligible prescriber requirements. Active medical staff who have clinical privileges are eligible to write 340B prescriptions. Specifically excluded from 340B prescriber eligibility are those physicians with admitting privileges only, affiliates, or emeritus staff. Practitioner information must be downloaded and frequently updated in the in-house dispensing system and also in the contracted pharmacy dispensing system by the hospital's credentialing department to help maintain the integrity of the data that is used by the pharmacy.

Table 3: Summary of Covered Entity Responsibilities with HRSA's Medicaid Exclusion File

Carve-In	Carve-Out
▶ Purchase drugs at 340B prices	▶ Purchase drugs at non-340B prices
▶ Medicaid patients receive 340B program drugs	▶ Medicaid patients do not receive 340B drugs
▶ 340B-purchased drugs are excluded from Medicaid Rebates	▶ Covered entity must respond with "NO" in the Medicaid Exclusion File
▶ Covered entity must respond with "YES" in the Medicaid Exclusion File	▶ No Medicaid billing numbers/NPI(s) are listed in the Medicaid Exclusion File
▶ Medicaid billing numbers/NPI(s) are listed in the Medicaid Exclusion File	▶ Covered entities must have clearly defined procedures surrounding the 340B process, monitoring, and auditing
▶ All listed NPI numbers must be checked for accuracy, especially to reflect any changes	▶ Covered entities must ensure compliance with state Medicaid Rebate billing procedures

Ensure 340B compliance with HRSA statute prohibitions

Duplicate discounts are prohibited and Group Purchasing Organizations (GPO) cannot use 340B discounts. During an HRSA or manufacturer audit, make sure policies, procedures, and other supporting documentation can be produced and align with the hospital's current practice.

A duplicate discount occurs when the same drug is purchased with an upfront 340B discount and also credited with a back-end Medicaid Rebate transaction. 340B hospitals are responsible for the prevention of duplicate discounts, and HRSA will request documentation to demonstrate compliance with the program.

When an eligible hospital enrolls in the 340B program, it must decide whether or not to purchase and dispense 340B drugs for its Medicaid patients (carve-in), or whether it will purchase drugs through other methods (carve-out). Table 3 summarizes these details. The decision as to how the 340B hospital will handle the dispensing of 340B drugs to Medicaid patients should be directly related to its diversion compliance plan.

When a hospital decides to purchase 340B drugs for its Medicaid patients, the hospital is required to inform HRSA by inputting its Medicaid provider number and/or it's National Provider Identifier (NPI) into HRSA's Medicaid Exclusion File database.

The Medicaid Exclusion File is the mechanism that state Medicaid agencies use to identify all covered entities that use 340B drugs for Medicaid patients, so that the state can remove pharmacy claims associated with those entities from rebate requests. The 340B hospital is responsible for its Medicaid Exclusion File accuracy, including all Medicaid billing numbers/NPI(s) used for billing those claims to the state.

If a hospital decides to bill Medicaid for drugs purchased under 340B with a Medicaid provider number/NPI, then all drugs billed to that number must be purchased under 340B and that Medicaid provider number/NPI must be listed on the HRSA Medicaid Exclusion

File database. When a hospital has multiple Medicaid billing numbers/NPI(s), it is possible that the hospital can decide which billing numbers (or facilities) dispense 340B-purchased drugs and which facilities do not.

The GPO prohibition is an eligibility requirement for DSH hospitals, children's hospitals, and free-standing cancer hospitals. Hospitals and their off-site outpatient clinic sites that are registered in the HRSA database are subject to the GPO participation prohibition and cannot purchase any covered outpatient drugs through a GPO or other group purchasing arrangement. Hospitals will attest to compliance with this prohibition annually at re-certification, and HRSA will review procedures and monitoring mechanisms to ensure compliance during an audit.

According to HRSA guidance, certain off-site outpatient hospital facilities may use a GPO for covered outpatient drugs, if those outpatient facilities meet all of the following criteria:

- Are located at a different physical address than the parent;
- Are not registered on the HRSA Database as participating in the 340B program;
- Purchase drugs through a separate pharmacy wholesaler account than the 340B participating parent; and
- The hospital maintains records demonstrating that any covered outpatient drugs purchased through the GPO at these sites are not utilized or otherwise transferred to the parent hospital or any outpatient facilities registered on the HRSA database.[5]

Because the GPO prohibition is an eligibility requirement, 340B hospitals found in violation will be considered ineligible and immediately removed from the 340B program. Hospitals may also be subject to repayment to manufacturers for the time period for which the violation occurred.

Tips for 340B program audit readiness

Developing a compliance plan and continually monitoring for compliance is an integral part of the hospital 340B program. Some essential oversight and monitoring components include:

- Plan for ongoing education for all levels of staff and physicians involved;
- Review and update policies to include all off-site clinics and contracted pharmacies;
- Update work process flows and re-evaluate the 340B standard operating procedures;
- Assess the impact of organizational changes (e.g., people, services, facilities) to ensure the HRSA database is accurate;
- Continually improve communication and flow of data and information;
- Develop a compliance plan that includes a self-auditing process;
- Conduct appropriate weekly, monthly, and quarterly monitoring for the various program elements;
- Plan for an external audit annually;
- Develop a community benefit plan to ensure intent of 340B program is supported; and
- Make sure the hospital has a procedure for when HRSA sends notification to initiate an audit.

Defend the intent of the program with a plan

Consider developing a community benefit plan in preparation for an HRSA audit to reduce the risk of the program's intent being questioned. Scrutiny over the original intent of the 340B program is increasing from lawmakers and drug manufacturers as the program has been experiencing unprecedented growth. There are concerns about the program's intent being shifted away from helping the low-income and uninsured populations to providing profit to large hospital systems.

The 340B program has nearly doubled in the number of participating sites since 2001 with 16,500 entity sites that were affiliated with

Register by August 18

SAVE $300

INCLUDES PRE-CONFERENCE FOR FREE

Clinical Practice Compliance Conference

OCTOBER 11–13, 2015 | PHILADELPHIA, PA

Why should you attend?

- Get updated on government initiatives specific to physicians and their practices
- Network with your peers
- Hear the latest enforcement trends
- Learn about correct documentation, billing and coding practices, and operating on a limited budget

Learn more at hcca-info.org/clinical

Questions: darin.dvorak@corporatecompliance.org

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

approximately 3,200 unique 340B entities in 2011. A recent study examined 960 hospitals and 3,964 affiliated clinics and found a difference in the population served from those sites registered before 2004 from those sites registered after 2004. The researchers concluded that when entities registered for the 340B program after 2004, the communities served were wealthier and had higher rates of having commercial health insurance. Some have questioned if hospitals are strategically locating outpatient clinics within more affluent, insured communities for the purpose of enhancing the profitability of the participating 340B hospital without advancing the core goals of the program.[6]

340B hospitals must meet certain eligibility requirements, as outlined above, based on their DSH percentage, which implies that those hospitals already do provide a disproportionate share of uncompensated care. 340B DSH hospitals continue to serve as the safety net for Medicaid, low-income Medicare, and individuals not eligible to purchase health insurance. Additionally, hospitals contend that the ACA encourages hospitals to shift inpatient care to outpatient settings, when appropriate, and be more accountable with coordinating care outside the walls of the hospitals. This shift in the marketplace is resulting in more hospital affiliations with more outpatient sites.

Currently under section 340B, there are no provisions related to how a covered entity distributes savings. According to a Government Accountability Office report, "…the purpose of the program is to enable covered entities to stretch scarce federal resources to reach more eligible patients, and provide more comprehensive services."[7] HRSA plans to issue more guidance concerning the 340B program within the next several months, and this topic will likely be discussed.

Hospitals should develop a community benefit strategy to address the allocation of savings, and how those monies will be used to enhance outpatient services for the low-income and uninsured populations. A community benefit strategy is not required by HRSA, but should be strongly considered.

HRSA plans to issue more guidance concerning the 340B program within the next several months…

Summary

The 340B program offers many benefits for hospitals to ensure their patients have continued access to outpatient services. The revenue gains associated with the 340B program should be strategically allocated throughout the hospital system to target those patients with the greatest financial need. Eligibility requirements for the program pertain to the hospital and not the financial status of the patients. Therefore, it is important for hospitals to demonstrate the community benefit of the 340B program on behalf of patients.

Hospitals must dedicate the proper resources to make sure that all 340B policies and procedures are adhered to, that oversight occurs continually, and that all pharmacies and outpatient clinics associated with the 340B hospital are well informed and compliant with the program requirements.

1. Public Health Service Act, 42 U.S.C. §256b.
2. Apexus: 340B Prime Vendor Program, informational sheet on the 340B Compliance for the C-Suite. Available at http://bit.ly/1yGBpEw
3. A.W. Mulcahy, C. Armstrong, J. Lewis, and S. Mattke: The 340B Prescription Drug Discount Program, Origins, Implementation, and Post-Reform Future. RAND Corporation, 2014. Available at http://bit.ly/1C4xTU6
4. Apexus, 340B University training session, October 2014. Available at http://bit.ly/1yGUqFg
5. Health Resources and Services Administration website at www.hrsa.gov/opa
6. R.M. Conti and P.B. Bach: "The 340B Drug Discount Program: Hospitals Generate Profits by Expanding to Reach More Affluent Communities." *Health Affairs*, 33 No.10 (2014): 1786-1792. Abstract available at http://bit.ly/1zutdac
7. U.S. Government Accountability Office, Report to Congressional Committees: Manufacturer Discounts in the 340B Program Offer Benefits, but Federal Oversight Needs Improvement. GAO-11-836, 2011. Available at http://1.usa.gov/1yGBSGR

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

The continuing saga of the Sunshine Payments Act

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

The Physician Payment Sunshine Act, a provision of the Affordable Care Act, was originally put in place to make financial relationships more transparent, give consumer's information to make informed decisions about their healthcare, and create a link to the fraud and abuse laws. When it was rolled out this past fall, it was fraught with problems. By initiating the Act, institutions and the industry were required to have a methodology for verifying fair market value to their contractual analysis process and to develop standard operating procedures (SOPs) regarding those procedures.

Willenberg

The industry itself is key to clinical trial research process, and they found themselves trying to develop a monitoring and tracking system for payments to sites or covered recipients. With varying sizes of sites, the tracking process was found to be complicated and time consuming. Language began to appear in contracts that sites would monitor and document all payments made by a research sponsor, and that they would transfer the documentation to the sponsor upon request. Sites have no obligation for reporting and sponsors cannot transfer liability to sites, so more confusion arose as sites began to question their role in the process.

Because the Act was planned to be "rolled out" in phases with differing requirements and varying timeframes, there were questions. During the implementation process though, it became apparent that there were challenges that industry, covered recipients, and the government would face. Some of those were anticipated, but much of what occurred was not.

Sites are now attempting to circumvent the issues they had not considered prior to the botched rollout. How does a site manage the review and verify or challenge reported payments? Who ensures that the physicians register in a timely fashion, so there can be a review of the reported payments? Since they cannot assume that the information posted is accurate, how do they perform detailed reviews to verify that the reporting is attributed to the correct category? During the rollout, it was discovered that many items were attributed to incorrect categories, such as travel and honoraria. Some data was reported under the wrong physician, and the list goes on. There are lingering questions for all involved in this process.

> Sites are now attempting to circumvent the issues they had not considered prior…

Finally, there are now questions from patients. Being prepared to answer those questions and who will answer them on the sites or physician's behalf needs to be identified. It is still unclear how many patients will access the database and why they will. Patients and their families may misinterpret the information when they access it. Having an infrastructure and plan is now, more than ever, necessary to deal with the "unknowns" of the Sunshine Payments Act.

SCCE Regional Conferences

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

Network & learn locally and earn CEUs

March 13, 2015 • Miami, FL

April 24, 2015 • Chicago, IL

May 1, 2015 • Washington DC

May 15, 2015 • New York, NY

June 19, 2015 • San Francisco, CA

June 25–26, 2015 • Anchorage, AK

October 23, 2015 • Minneapolis, MN

October 30, 2015 • Atlanta, GA

November 13, 2015 • Boston, MA

December 4, 2015 • Dallas, TX

corporatecompliance.org/regionals




by Emmelyn Kim, MA, MPH, CCRA, CHRC and Tina Chuck, MPH

Five tips for success in research compliance education

» Create an organizational structure around education and training.
» Integrate all aspects of research compliance.
» Build partnerships, collaborate, and use a multi-disciplinary approach across departments.
» Use flexible adult learning methods in training programs.
» Continually evaluate your program with metrics for improvement.

Emmelyn Kim *(ekim@nshs.edu) is Director, Research Compliance and* ***Tina Chuck*** *(tchuck@nshs.edu) is Manager, Research Policy and Training, both in the Office of Research Compliance and Research Policy and Training at North Shore-LIJ Health System in New York.* /in/EmmelynKim /in/TinaChuck

The regulatory environment of research is often complex and ever changing, which is why education and training are vital components of research compliance. However, implementing and sustaining a successful research education and training program can be challenging due to the myriad of research activities occurring from the laboratory to the clinical space. Therefore, having a dedicated education and training program has become more of an essential component, rather than an option, for our organization. The following are tips to consider for establishing your program and are based on our program and experience at the North Shore-LIJ Health System.

1. Create a solid program foundation

The Office of Research Compliance (ORC) at North Shore-LIJ has been involved in providing education and training for researchers since the inception of the program approximately ten years ago. During the infancy of the program, compliance staff would hold "research cafes" to provide regulatory updates and guidance on application for researchers. Other research administration departments would hold their own education sessions, but such efforts were independently communicated and sometimes not known to other departments. Education was also the responsibility of staff from various departments, but most had only 5%–10% of time dedicated to these activities and therefore, some programs were more developed than others.


Kim


Chuck

Over time, it became clear that a central infrastructure and dedicated personnel were needed to streamline research regulatory communications and assist in developing and distributing policies as part of an effective research education and training program. At North Shore-LIJ, the Office of Research Policy and Training (RPT) was created to centralize all education and training efforts and has two full-time employees (FTEs) dedicated to the program. This foundation has allowed us to build a more comprehensive and effective program that ties education, training, and policy together in a seamless fashion.

2. Employ a holistic view of research

When thinking about your research program's needs, consider all the spaces and employees that research activities may touch, from

laboratory/preclinical to the clinical areas and administrative offices. Research may occur throughout the various research laboratories, offices, patient care areas, and teaching facilities. However, when you think about the various aspects involved in research, this may include grants and finance, technology and materials transfer, safety, protocol development, regulatory approval, recruitment, study conduct, data/sample collection and analysis, investigational products, etc.

Your program should cover the entire spectrum of research occurring at your institution, because researcher education and training needs will vary based on activity and role. For example, laboratory scientists, residents, principal investigators, and research coordinators may require different types of education and training, and they need to understand how to navigate through different administrative offices. Laboratory personnel may need more extensive training on safety, but clinical personnel may need more training on HIPAA privacy and security. Finally, the geographic location of research activity is an important consideration for our diverse health system that is spread across the boroughs of New York City and Long Island. Each location will vary in terms of research needs based on their portfolio, population, experience level, culture, and infrastructure. All aspects of research should be considered to effectively develop a comprehensive program that can engage and benefit everyone in your research community.

Your program should cover the entire spectrum of research occurring at your institution…

3. Build a team of content experts

The development of research education and training programs that comply with regulatory, industry, and institutional policies and standards involves the collaboration of content experts from multi-disciplinary departments. RPT works with various departments within Research Administration and across the health system (e.g., ORC, Grants Management, Legal Affairs, the Human Research Protection Program [HRPP], Tech Transfer, Safety, Biostatistics, Animal Care and Use Program, Clinical Research Services, Information Services, etc.) that inform the creation of our programs. Within the different departments, we have partnered with select people who are content experts in their area of expertise and inform the development of training materials as part of their job function. We also seek the opinion of leaders in research training from other academic institutions and research organizations. Building a rapport with content experts takes time, but the time invested in establishing these partnerships paves the way for successful training programs.

In order to sustain partnerships with content experts, it is important for everyone to see the value added to research training programs when using a collaborative approach for development. Benefits we have seen include the reduction of frequently asked questions that research administration offices receive and increased competency of researchers after completion of training programs. Management has seen faster turn-around time for the delivery of training programs that integrate all aspects of research compliance with the input of content experts. Working with the various departments keeps our research training programs and materials current and up to date. It would be impossible for a professional trainer, or even a team of trainers, to be knowledgeable of all the changes that need to

be made without input from content experts. This method enables timely introduction of new institutional policies and procedures consistent with regulatory changes that serve to reduce research compliance risk.

4. Be flexible and offer variety

When we think of research training, we often picture no frills PowerPoint lectures or online courses. However, adults learn differently than children, and there is no "one size fits all" format for training. RPT has found that the best "fit" is to offer multiple formats for training, including in-person, online, and live telecast options. All of our formats incorporate adult learning methods in an effort to maximize the knowledge retention of the learners and also to help apply the knowledge in daily research scenarios. We utilize training tools that appeal to people who are visual, aural, and actionable learners. Supplemental training materials (e.g., handouts, diagrams and pictures, case studies, videos, and guidance documents) are used to reinforce the objectives that are being taught.

The introduction of learning technologies has been beneficial to our training programs. North Shore-LIJ uses a learning management system to administer training and education. This allows research compliance education to be easily tracked and managers can run reports to manage research staff training. Managers are also able to assign in-person and online research training as part of corrective action plans or professional development. Other technologies include an audience response system and e-learning development software. The audience response system is incorporated into PowerPoint presentations and is able to capture real-time data by having learners answer polling questions. This is a great way to gauge learners' knowledge before, during, and after training presentations and can drive what objectives need more attention. The e-learning development software permits us to create interactive online trainings and quick instructional videos that learners can complete at their own pace. Using this software, we can engage learners by having them apply knowledge through interactive games, quizzes, and videos.

We offer a mix of centralized training programs as well as custom tailored trainings that might be role, facility, or department specific. Centralized trainings are scheduled regularly (i.e., weekly, quarterly) throughout the year at set locations that are set-up to provide an environment outside of the office that encourages interactive discussion. For example, tables are arranged in classroom style for workshops, with dry-erase walls for group exercises and proper audio-visual equipment. Custom-tailored trainings are created on an as-needed basis. They can be requested by a research team for a specific topic or be planned as part of a corrective action plan as a result of an ORC audit. Content experts perform many of the trainings; hence, it is important to remain flexible and have a coordinated effort to facilitate the right type of training when needed.

5. Evaluate and improve your program

Using metrics for evaluation is necessary to continuously make improvements to achieve research compliance education success. Many of our research training programs offer continuing medical education (CME) and continuing education unit (CEU) credits and must comply with standardized evaluation criteria that are established by the Accreditation Council for Continuing Medical Education (ACCME) and the International Association for Continuing Education and Training (IACET). Standard evaluation methods include having attendees complete evaluations (in-person and online) after the completion of a training. These evaluations provide feedback from attendees on whether or not the training met their learning needs, the format of the training, and the effectiveness of the presenter.

For CME-approved training programs, we also follow up with an outcomes evaluation that is sent via email to participants three months after completion of the training. The purpose of the outcomes evaluation is to assess whether or not the learners implemented any of the knowledge from the training into their daily research practices. Metrics from both types of evaluations include data on number of attendees, overall rating of the objectives, overall rating of the presenter, assessment of new information that was learned, and suggestions or comments. Other metrics are gathered from research reviews and audits conducted by the ORC, which provide insight on research performance, conduct, and quality. These metrics are shared with leadership and are used to inform future development or revisions to education, training, and policies.

Conclusion

The tips outlined in this article enable you to implement critical steps (e.g., planning, support, and evaluation of your program) in partnership with other departments and researchers. As the research landscape becomes increasingly regulated and complex, it is vital that institutions proactively build effective education and training programs to reduce the compliance risks to the organization while supporting research efforts. Continual integration of new regulatory trends and issues in trainings will serve to promote safe, compliant, and optimal research practices. Lastly, a successful program will enhance communication and enable departments and researchers alike to become more proficient in identifying institutional resources and more efficient in carrying out all aspects of research.

Don't forget to earn CEUs for this issue

Complete the *Compliance Today* CEU quiz for the articles below from this issue:

- **Compliance challenges in new chronic care management code**
  by Peter A. Khoury (page 39)
- **340B drug program: Hospital audit readiness**
  by Susan Prior and Cristine Vogel (page 43)
- **The talisman to ward off worthless services cases**
  by Pamela Duncan (page 65)

To complete a quiz: Visit *www.hcca-info.org/quiz*, log in with your username and password, select a quiz, and answer the questions. The online quiz is self-scoring and you will see your results immediately.

You may also email, fax, or mail the completed quiz.

EMAIL: ccb@compliancecertification.org

FAX: 952-988-0146

MAIL: Compliance Certification Board
6500 Barrie Road, Suite 250
Minneapolis, MN 55435
United States

To receive one (1) non-live CEU for successfully completing the quiz: You must answer at least three questions correctly. Only the first attempt at each quiz will be accepted. Each quiz is valid for 12 months, beginning on the first day of the month of issue. Quizzes received after the expiration date indicated on the quiz will not be accepted.

Questions: Call CCB at 888-580-8373.

by Kim Keehn, MS, LPC

Preventing and detecting fraud and abuse in a managed care network

» Data mining is essential to detecting potential fraud and abuse in a network of providers.
» A cross-functional team using open communication is vital to the success of a compliance program.
» Implementing various program integrity strategies is the most effective way of eliminating fraud and abuse.
» It is important to have various means for reporting suspected fraud and abuse and providing education about those reporting methods.
» Reporting suspected fraud and abuse is the responsibility of everyone.

Kim Keehn *(kdkeehn@ecbhlme.org) is the Senior Director of Quality and Compliance for East Carolina Behavioral Health in Greenville, NC.*

East Carolina Behavioral Health (ECBH) is a Local Management Entity/Managed Care Organization designated by the North Carolina Department of Health and Human Services to oversee the appropriate provision of state and federally funded Behavioral Health and Intellectual/Developmental Disability services and support in 19 counties throughout eastern North Carolina. Through a contract with the North Carolina Division of Medical Assistance (DMA), ECBH is responsible for conducting program integrity activities to ensure that dollars are spent in a way that complies with federal and state mandates. These activities include monitoring provider billing practices to ensure these funds are used to purchase appropriate, quality care for individuals needing services. ECBH utilizes various techniques and processes through a cross-departmental approach to conduct this type of monitoring.

Keehn

Fraud and abuse management system

In December 2013, ECBH began utilizing a fraud and abuse management system[1] to detect potential fraud and abuse, or questionable business practices, within its provider network. This data mining system uses behavioral modeling to detect common fraud and abuse schemes. It was first implemented by the North Carolina Division of Medical Assistance in June 2010 and has contributed to major fraud, waste, and abuse identifications across many areas in the state. The models are configured to North Carolina Medicaid and are frequently updated based on experience, environmental changes, provider behaviors, and time. This system uses over 9,000 algorithms and models used across healthcare industries with both public and private payers.

This system detects suspicious providers and associated claims by using advanced analytical tools that are able to identify which providers are behaving differently than others, patterns of non-compliant behavior, or groups of providers behaving the same. The system then predicts which providers are likely to be non-compliant in the future.

Every month, ECBH is able to develop and review reports that are specifically designed to target possible issues for review. These reports explain, in a clear and concise manner, the reason a provider was detected and provide supporting documentation to allege a behavior of non-compliance. This way, staff are deployed to review only the claims with the highest probability of improper payment. Some of the issues that these reports identify include possible overbilling, billing for services not rendered, unbundling services, and back filing. However, it is important to remember that detection through these reports only identifies a *potential* issue and is not proof of a violation. A thorough review of the results is always warranted before any action is taken. Therefore, these reports are first reviewed by an internal Program Integrity Committee (PIC) to determine if further action is warranted.

Program Integrity Committee

A PIC is designed and used as a way to detect and prevent fraud and abuse within the network of behavioral health providers. ECBH maintains a committee that is comprised of a cross representation from various departments, including Quality Management, Network, Call Center, Information Management, Utilization Management, and Claims/Finance. Many of the committee members have completed the National Certified Investigator and Inspector Training (NCIT) through the Council on Licensure, Enforcement, and Regulation (CLEAR).[2]

This committee meets on a monthly basis to review reports, complaints, and current investigations on questionable practices by providers. The questionable business practice information is received from various sources, such as internal staff, an anonymous reporting hotline, complaints from providers in the network, an access-to-care line, website submissions, mail, and reports from the North Carolina Department of Health and Human Services.

In addition to reviewing individual complaints and allegations involving potential fraud and abuse, the committee also reviews aggregate claims data from internal reports, as well as reports from the fraud and abuse management system, to identify patterns, trends, and possible outliers. Concerns are referred to the Network department for further investigation and possible referral to the Program Integrity Unit with the North Carolina DMA. All program integrity activities are logged and reported to DMA on a monthly basis, including the number of investigations being conducted, the outcome of investigations, and any recoupment of Medicaid dollars.

Explanation of Benefits

An Explanation of Benefits (EOB) form can be used as another strategy to identify potential fraud and abuse. ECBH utilizes this strategy by sending out 100 forms to Medicaid recipients on a quarterly basis to inquire about the services they have received. The form surveys the recipients about the following questions:

- Did you receive this service from the provider?
- Did this provider bill you for this service?
- Did you pay this provider for the service?
- Do you have any other Health Insurance

These EOB forms can be targeted to individuals who are receiving services from a specific provider or group of providers that have been identified as having suspicious billing activity from the reports generated by the fraud and abuse management system. EOB forms that identify a potential problem are reviewed by the PIC to determine if a referral for investigation is necessary.

Reporting hotline

Confidential, toll-free hotline numbers can be made available to all employees, providers, contractors, and vendors, as well as interested outside parties, as a way to receive tips on potential fraud and abuse occurring in a provider network. ECBH utilizes a hotline number that

is designed to supplement existing reporting channels for questionable business practices in the network. Hotline calls are not recorded or traced, and callers may remain anonymous if they so desire. All employees, contractors, and vendors are encouraged to call the Compliance Reporting Hotline to ask questions or seek guidance regarding specific activities. All calls are treated in a manner that is confidential, but also consistent with the need to investigate, cooperate with the government, and comply with legal obligations. All calls regarding potential fraud and abuse are investigated promptly.

Summary

ECBH, as a managed care organization, is not able to make a determination as to whether activity by a behavioral health provider is, indeed, fraudulent. Suspicious billing practices that are discovered are referred to the Program Integrity Unit at DMA, with supporting documentation, for a determination to be made as to whether fraud and/or abuse has occurred. Referrals that are accepted are then referred to the North Carolina Medicaid Investigation Division for further review and possible investigation.

Utilizing a variety of tools and strategies is an efficient and effective way to detect, prevent, and eliminate the occurrence of Medicaid fraud and abuse in behavioral health services. In fiscal year 2014, ECBH conducted a total of 38 investigations into potential fraud and abuse as a direct result of these program integrity activities. From those investigations, over $250,000 in Medicaid funds was recouped from providers (some recoupments are still in the appeal process) and put back into services for individuals in eastern North Carolina.

1. IBM Global Business Services: IBM Fraud and Abuse Management System website. Available at http://ibm.co/15938QA
2. Council on Licensure, Enforcement & Regulation: National Certified Investigator and Inspector Training website. Available at http://www.clearhq.org/NCIT

HCCA Training Resources

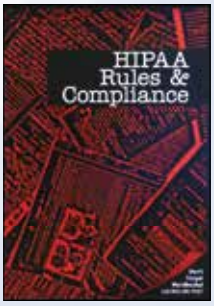
GUIDEBOOKS & VIDEOS TO TRAIN YOUR HEALTH CARE WORKFORCE

Compliance and Ethics: An Introduction for Health Care Professionals

HCCA's top-rated DVD covers 7 key compliance areas in a 23-minute program split into 7 dramatized scenarios. Includes a trainer's guide with suggested agendas and discussion outlines.

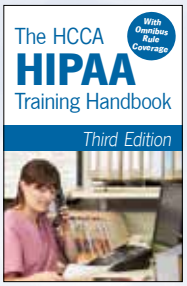
Compliance, Conscience and Conduct

HCCA's classic compliance training DVD is still available! The 17-minute video overviews what compliance means and walks viewers through seven common case studies. Includes session leader guide and reproducible participant worksheets.



HIPAA Rules & Compliance

This 15-minute video reviews basic, unchanged requirements and the latest, critical changes, including the Omnibus Rule.



The HCCA HIPAA Training Handbook, Third Edition

The new, third edition of this handbook covers the privacy and security regulations that frontline health care workers need. This 40-page primer clearly explains the essential, basic workings of HIPAA, HITECH, and the Omnibus Rule.

A Supplement to Your Deficit Reduction Act Compliance Training Program

This 13-page handbook offers an easy way to educate your employees about the basics of Medicare and Medicaid, the Federal False Claims Act, and the whistleblower protections that help health care workers fight fraud.

Workplace Investigations: Techniques and Strategies for Investigators and Compliance Officers

Get step-by-step guidance for planning, conducting, and reporting results of internal investigations.

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

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

by Jillian A. Watts, Esq., CHC

The Physician Payment Sunshine Act: Lessons learned in the first year

» Registration for the Sunshine Act began July 14, 2014 for physicians and teaching hospitals.
» The registration process was frustrating and time consuming.
» The dispute resolution process was difficult to navigate.
» Data became publicly available on September 30, 2014.
» The data available did not paint a complete picture.

Jillian Watts *(jawatts@bidmc.harvard.edu) is a Conflict of Interest Specialist with Beth Israel Deaconess Medical Center in Boston.*

In February 2013, the final regulations for the Physician Payment Sunshine Act, commonly referred to as Open Payments, were released in the Federal Register.[1] The Sunshine Act requires manufacturers of pharmaceuticals, devices, and biologics to track and report payments and transfers of value made to licensed physicians and teaching hospitals to the Centers for Medicare & Medicaid Services (CMS). Physicians and teaching hospitals are referred to as covered recipients in the regulations. The final regulations required CMS to publish all of this data on a public database by September 30, 2014.[2] On the path from the release of the final regulations to the public release of the data, several lessons were learned.


Watts

Education was critical

Covered recipients were supposed to have a 45-day period, from July 14 – August 27, to create a log in, privately review the information reported about them, and resolve any disputes about the reports. Many organizations tried to get the word out to their medical staff, so that they didn't miss this opportunity.

Live presentations were the best way to reach the physicians. Most physicians are incredibly busy and simply do not have the time to sort through their abundance of daily emails. Presenting at their faculty meetings assured that they would at least be present and, hopefully, listening.

In addition to live presentations, email blasts and webinars were also used. Once a physician has a face to go with a name, they are more likely to open an email from that individual. Emails were also an important tool when trying to communicate key dates to the leaders of a hospital who may not have time for even a 15-minute meeting.

Registration was anything but smooth sailing

The registration process was broken up into two phases for covered recipients. The first phase of registration started on June 1, 2014 and allowed physicians and teaching hospitals to gain access to CMS's Enterprise Identity Management system and the CMS Enterprise Portal. The next phase of registration began

slightly over a month later, on July 14, and allowed access to the Open Payments system.

Phase One of registration was not too difficult. The most common complaint was from physicians who did not know how far in the registration process they could go, which seemed to vary from physician to physician. Ultimately, the main reason the first phase of registration went smoothly was because most physicians did not try to register. CMS should have had only one phase in the registration process.

Unfortunately, Phase Two of the registration process did not go as smoothly. The first complaint was that CMS hid the directions for registration in the middle of a 361-page User Guide.[3] If a physician does not have time to read all of their daily emails, they certainly do not have time to sort through a 361-page guide to figure out how to register. An email was sent on behalf of the Medical Executive Committee to all physicians in our Medical Center notifying them that registration for Phase Two had started, and provided them with simple step-by-step instructions. As the phone calls and emails started overflowing, we quickly realized that more was required than a few simple instructions.

A step-by-step guidance document with screenshots for each step was created and circulated to all physicians. Physicians were also instructed that certain internet browsers would not support the Enterprise Portal. Unfortunately, at our Medical Center, the standard browser found on each desktop was not supported. Many physicians were advised to try registration on their personal computer.

Physician registration required their taxonomy code, National Provider Identifier (NPI), and state license number. Again, the taxonomy code was buried in another document presented by CMS.[4] Some physicians also did not know their NPI number. This was a problem, because after 15 minutes of inactivity, the Enterprise Portal would boot a user out of the system. Most physicians indicated that they gave up trying to register after several hours of failed attempts.

Some teaching hospitals also hit a bump in the road early on in the Phase Two registration process. Some physicians were able to register themselves as the Authorized Official of a teaching hospital. This happened to at least two hospitals. This was a problem for two reasons. One, the physician could see all of the data that was being reported under the hospital's name. Additionally, no one else from the hospital could gain access to the system unless either the physician approved the request for access, or CMS went into the system and removed the physician as the Authorized Official. Working hand-in-hand with CMS was the only way to have the physician removed as the Authorized Official. Meanwhile, the dispute resolution process was running concurrently with Phase Two registration.

Some teaching hospitals also hit a bump in the road early on in the Phase Two registration process.

Dispute resolution was not so clear

After spending anywhere from minutes to days completing the registration process, covered recipients could finally see what manufacturers were reporting under their name. Three options were available: attest, dispute, or do nothing. Our Medical Center decided to dispute what it needed to, and do nothing with any other data. There was no clear indication what an attestation would do down the road. The next step was to try to navigate the data and sort it in some manageable way. The Open Payments database did not allow for any data to be downloaded. With some technologically savvy assistance, some teaching hospitals found ways to download the data. This step

was much more critical for hospitals that have hundreds of line items to review.

Disputes were then initiated. Problem one arose: The text box for a dispute does not allow the user to enter numbers or certain other special characters. This becomes a problem when CMS insists that the dispute resolution process is strictly between the manufacturer and covered recipient, and does not provide either party with any contact information. Eventually, some academic medical centers spread the word that the best method was to spell out a phone number and use AT to communicate an email address in the text box. "Call Tom at eight six seven five three zero two, or email tomATemailaddress.com."

Additionally, CMS shut the entire Open Payments system down for almost two weeks in August. Some physicians were able to see payments made to other physicians with the same name. CMS responded by removing all payments that could be connected to multiple physicians, approximately one-third of all payments reported. When CMS opened the system back up for the remainder of the review and dispute period, several hospitals reported having payments previously reported under their institution removed. Even some payments that were identified prior to the shutdown were removed from the system.

The next problem arose when emails came from CMS stating that a manufacturer had resolved a dispute. How could a manufacturer resolve a dispute when the covered recipient had not received any communication from a representative of the manufacturer? CMS had stated that errors had to be resolved between the covered recipient and the manufacturer. However, manufacturers were given the ability to unilaterally resolve disputes. If the manufacturer thinks its initial report is accurate, they can resolve the dispute as being resolved with no changes, without ever speaking with another person.

Under the regulations, payments are classified as either being for Research, General Payment, or Ownership. There are several Nature of Payment categories under General Payments.[5] Manufacturers were using the Nature of Payment categories inconsistently. Some would call a fellowship a grant, while others would call it education, and still others would call it "payment for services other than consulting." This was particularly troublesome for the Services Other Than Consulting category. The regulations state that this includes services provided by a physician or teaching hospital to a manufacturer and may include marketing or promotional activity.[6] Fellowships are educational and provide no deliverables to the manufacturer that may be supporting it. Fellowships are certainly never promotional in nature. Accordingly, fellowships should have been categorized as either education or a grant. Some payments were also reported under General Payments when they should have been under Research. This was particularly true for materials provided under a research grant that were being categorized as in-kind payments under the General Payments category.

The next problem arose when emails came from CMS stating that a manufacturer had resolved a dispute.

We had anticipated that dispute resolution would be difficult, given the number of covered recipients and manufacturers involved across the nation. To our pleasant surprise, once contact was made between the parties, the dispute resolution process worked fairly well, as both parties were interested in accurate reporting. It appears that both CMS and manufacturers had adequately staffed their contact desks.

Finally, some physicians were having research payments reported under their names, when the payments should have been attributed to a teaching hospital that actually received the funds or materials. This incorrectly places a very large dollar value next to a physician's name. This could lead to confusion when a patient is trying to navigate the data and sees a large payment incorrectly reported under their physician's name. All research payments or materials provided under a research agreement to a teaching hospital should have been attributed to the hospital. The physician's name should only appear when they are the principal investigator (PI), and PIs should not have any payment attributed to them personally.

We are live!

On September 30, 2014 the data became publicly available. Initially, the data was presented in a manner that was not quite user friendly. Over time, CMS has updated the search functions, which has made the data more navigable. All of the data is available for download, which is beneficial for a hospital searching for payments for a certain physician or trying to compare payments made to other hospitals.

The main question that remains unanswered is: Where is all of the data? CMS published a fact sheet explaining that large amounts of data were published without identifying who the recipient of the payment was.[7] According to CMS, approximately $2.2 billion worth of data was published without an identifier.[8] Any payment that was disputed and not resolved was not reported in the first release of the data. Other payments were not identified, because CMS indicated there were errors on behalf of the manufacturers. Manufacturers have since received their data that was published without identifiers and have until the end of the next data submission period to correct and resubmit this data. This has left an incomplete picture for the first, short reporting year of Open Payments.

What can we expect going forward?

Next year will bring a full year of data to review and sort through. Payments have been tracked by manufacturers from January 1, 2014 through December 31, 2014. It is anticipated that there will be millions more lines of data for manufacturers to submit and covered recipients to review. Because registration is ongoing, the registration process should move more smoothly. Perhaps CMS will address some of the functionality issues in the dispute resolution process. Ideally, contact information for the manufacturer that reports the information would be provided, and when a dispute is initiated, a covered recipient should be able to type numbers and special characters into the text box. This will allow for communications to start more quickly and be more efficient. Additionally, manufacturers should not be able to unilaterally resolve any disputes. Communication is the key to success with Open Payments.

Looking ahead

With a full year of data becoming publicly available on June 30, 2015, the attention to the data will be much greater. The government will be sorting through the data. Additionally, the media will most likely cover the next data release in more depth. If the process goes any smoother than the first data release, the media will most certainly be focused on the dollars being reported, and not on the flaws of the system.

Some faculty members have expressed apprehension at appearing on the public database. One can only hope the influx of attention sure to occur on June 30, 2015 will not create a chilling effect on the beneficial and necessary relationships that occur between manufacturers and physicians and teaching hospitals.

1. Centers for Medicare & Medicaid Services: 42 CFR Parts 402 and 403, 78 Fed. Reg. 9457; February 8, 2013. Available at http://go.cms.gov/1uBDqNx
2. *Id*.
3. Available at http://go.cms.gov/1J91vQb .
4. Available at http://go.cms.gov/1yEJKFw .
5. 42 C.F.R. §403.904(c)(7),(e)(2), 78 Fed. Reg. 9475
6. 42 C.F.R. §403.904(e)(2)(ii), 78 Fed. Reg. 9480
7. Available at http://go.cms.gov/1yGUPYr
8. *Id.*

by Pamela Duncan

The talisman to ward off worthless services cases

» Worthless services cases generally stem from prolonged, substandard conditions.
» Defending a worthless services case is complicated, expensive, and arduous.
» Vibrant quality assurance committees help stave off worthless services claims.
» Effective quality assurance is comprehensive, collaborative, and improves outcomes.
» CMS-mandated quality assurance programs include five specific elements.

Pamela Duncan *(pduncan@agapesenior.com) is the Chief Compliance Officer with Agapé Senior in Columbia, SC.*

In recent years, the healthcare profession, particularly skilled nursing, has seen a rise in the number and the severity of what have been deemed "worthless services" cases. Such cases stem from an assertion that the quality of care provided to patients can be so far below the expected standard of practice that they are, essentially, worthless. As such, any claims billed to and paid by the Medicare program for those services are being arguably considered to be false claims.

Duncan

Defending the case

Defending a worthless services claim is a perilous, uphill battle for a healthcare organization. Even with excellent care and services delivered to their patients, defending such a case inflicts upon an organization tremendous expense and significant interruption to business due to a burdensome and intrusive discovery process. Particularly in the skilled nursing setting, the patient population is somewhat aged and is usually experiencing both acute and chronic health conditions. Comorbidities and the effects of aging on the body often cause progressive health decline, which would be irreversible, even in the best possible care conditions. The care of such patients is presented to a jury, with inflammatory and differing opinions about what the services should have been. The jury is then asked to make a subjective judgment about the quality of the services delivered.

Compounding the difficulty in proving, years after the fact, that appropriate care was provided, is the relative ease of filing a worthless services case. Unlike wrongful death suits or malpractice cases, where the injured party files the claim, worthless services cases may be filed by anyone claiming to have knowledge of the care provided by the entity. Additionally, under *qui tam* procedure, the person bringing the case stands to gain a significant share of the monetary recovery, even into millions of dollars. In short, worthless services cases are easy to file, difficult and expensive to defend, and may be very lucrative to the initiator if a monetary settlement is reached.

Defending worthless services

Adding more challenge to the ability to defend is that the very concept of worthless services is not well-defined. Recent cases, from different districts, have provided the industry with mixed definitions of exactly what may constitute worthless services. In a skilled nursing

case from 2013, the court defined worthless services for the jury as:

> Services that are so inadequate, deficient, and substandard, or so completely lacking in value or utility to a nursing facility patient, that a reasonable person would understand that any services provided were worthless. Services can be worthless, and the claims for those services can, for that reason, be false, even if the nursing facility in fact provided some services to the patient. To find the services worthless, you do not need to find that the patient received no services at all.[1]

The jury in that case was further instructed that examples of conditions that may constitute worthless services may be:

- Inadequate staffing
- Improperly maintained equipment
- Inadequate supplies and equipment
- Improper decubitus ulcer care (bed sores)
- Inadequate pest control
- Improper accounting for resident trust fund accounts
- Dysfunctional governing body

More recently, in an appeal[2] overturning the ruling in the same case (decided in August 2014), further instruction narrowed the definition considerably, stating, "performance of the service [must be] so deficient that for all practical purposes it is the equivalent of no performance at all." Further, "[i]t is not enough to offer evidence that the defendant provided services that are worth some amount less than the services paid for. That is, a 'diminished value' of services theory does not satisfy this standard." The court concluded that, simply put, "services that are 'worth less' are not 'worthless.'"

To better identify exactly what does constitute worthless services, it is perhaps easiest to look at the circumstances that existed in facilities that were not successful in defending their cases. In looking at common themes from the recent worthless services cases, one strong component surfaces: a prolonged, substandard condition or conditions, of which the leadership was aware, that did not get corrected or improved. Issues in these cases ranged from environmental cleanliness, to inadequacy of supplies or food, to proper management of clinical conditions.

Although the specific circumstances change from case to case, the prolonged and unimproved nature of the issues is the most prevalent concern. Successfully defending a worthless services case, then, may very well start with one fundamental thing: an effective quality assurance/performance improvement program.

The elements of quality assurance

For a healthcare organization's quality assurance program to be effective, it must be more than a policy manual stuck on a shelf and a meeting once a quarter. It must be comprehensive, collaborative, and committed to improving systems and outcomes. An effective quality assurance program is made up at least the following five components:

1. Written policies and procedures
2. Leadership
3. Benchmarking and monitoring
4. Improvement projects
5. Evaluating effectiveness

The first element, policies and procedures, should specifically describe the framework and functioning of the program. The policies should detail the program's breadth and depth, as well as how the program will be integrated into the care and services being provided. The policies should outline the goals of the program and how the organization will select and monitor key performance indicators. Finally, the policies and procedures should describe the exact process the center will use to implement and monitor performance improvement activities.

The second element, leadership, speaks to the role and responsibilities of leadership on two levels: within the quality assurance team and the organization's governing body. The program must involve a commitment by leadership, at both levels, to allocate the time and resources necessary to fully develop and implement an effective program. Further, the written quality assurance plan should specify the individual(s) ultimately responsible for the improvement activities within the organization, including on-going education, quality assurance meetings, documentation of the overall quality assurance activities, and how communication will occur between the quality assurance team and the governing body.

…not only substandard quality areas may be targeted… rather, well-performing areas, which could be performing even better, can and should be improved.

The third element, benchmarking, encompasses the specific systems the quality assurance team utilizes to measure and monitor the outcomes of the care and services delivered. This element identifies the items and areas that will be monitored and measured, the frequency of the measurements, and the methods of benchmarking those measurements (comparing against own performance over time, against national standards, etc.). Finally, essential to this element, is the effective communication of the data analysis within the quality assurance team and to their governing body.

The fourth element of an effective quality assurance program is the fundamental improvement process itself. When the quality assurance team, through its benchmarking and monitoring, observes an area where performance could be improved, the leadership of the organization must devote the time and resources necessary to analyze the issues, identify the causes, and implement systematic changes that will improve the performance of that area. It is important to note that not only substandard quality areas may be targeted for quality improvement action plans; rather, well-performing areas, which could be performing even better, can and should be improved.

The fifth and final element of the program is the evaluation of the effectiveness of both the program itself and of the performance improvement projects that have been undertaken. Within this element, the quality assurance team reassesses issues, after the performance improvement plans have been completed, to verify that such activities were successful in bringing about the desired result. Further, in this element, the quality assurance team regularly evaluates the effectiveness of its own quality assurance program, as a whole, in developing a culture of continual improvement within the organization.

Conclusion

Simply noting in the quality assurance program that there are problems or issues is not enough to satisfy the purpose or intent of the program and not enough to serve as a defense in a worthless services case. The ultimate purpose of identifying and monitoring key performance indicators is that they be steadily improved. An effective performance improvement program, that meets its purpose and is complete with all five elements, serves to powerfully refute allegations of deliberately ignoring or recklessly disregarding areas of substandard quality.

1. U.S. ex rel. Absher v. Momence Meadows Nursing Center, Inc., No. 04-2289 (C.D. Ill.)
2. U.S. Court of Appeals, Seventh Circuit: *re Absher v. Momence Meadows Nursing Center , Inc.* Available at http://bit.ly/152A8uG

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 Lisa I. Wojeck, MS, JD, CFE, CISA, CHC

HIPAA Security Rule system activity reviews

» The HIPAA Security Rule requires system activity reviews occur regularly.

» The HIPAA Security Rule requires covered entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems containing or using ePHI.

» Identify a leader to own the system activity review process.

» Accounting and audit configurations must be appropriately set to capture system events.

» System activity review reports must be reviewed in context with other pertinent data.

Lisa I. Wojeck *(lwojeck@fpi.umaryland.edu) is Associate Director of System Integrity and Regulatory Compliance, University of Maryland Faculty Physicians, Inc., Faculty Practices of the University of Maryland School of Medicine in Baltimore.*

On a regular basis, we hear about breaches of electronic protected health information (ePHI). Although the breaches are all disturbing, it's those that occur from inside the organization that cause me greater concern. Specific sections of the HIPAA Security Rule (hereinafter, the Rule) instruct covered entities to: (1) implement policies and procedures to regularly review records of system activity[1] and (2) implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.[2]

Wojeck

In essence, the Rule requires both detective and preventive controls so employees know that their interactions with ePHI may be scrutinized and questioned, and disciplinary action may result. Employees who may be tempted to wrongfully access ePHI may be deterred.

Reducing the risks

The following six questions will help you design an effective system activity review to reduce the risk of a breach caused by insiders.

Who is responsible for these reviews?

The hard part is determining who is responsible for these reviews. Legal departments are often focused on moving contracts and business ventures forward, and potentially responding to claims. Compliance departments may be focused on coding reviews and training. Furthermore, Legal and Compliance departments may not have the skill set or desire to understand information services and technology. Along the same thought process, Information Services and Technology (IS/IT) departments may not be comfortable reading and interpreting the Rule.

Nevertheless, someone needs to own and lead this endeavor. Ideally, this person is comfortable with the Rule, information systems, and technology and is able to work collaboratively with Compliance, Legal, IS/IT, and the Human Resources departments.

Are systems configured appropriately?

With the advent of electronic health records, IS/IT departments at covered entities should verify that the accounting and audit configurations are set appropriately to ensure system events are recorded for all systems that store, access, or transmit ePHI. Events must be recorded in real time as they occur.

The events selected for the audit trail may be captured at the network, operating system, and/or application level. At a minimum the following should be captured:

- Who and/or what accessed the information or system?
- At what time and date was the information or system accessed?
- What information or system was accessed?
- What action or event occurred? (e.g., Was a file read, modified, or deleted? Was there a connectivity issue?)

Accounting and audit records must be stored in a secure manner.

Has a breach occurred?

How do you know if system activity review reports are revealing a potential breach? Looking at system activity review reports may not reveal a problem at first glance. These reports may not reflect the full picture and may need to be reviewed in context with other data. For example, while an employee may have appropriate access to all ePHI within his/her department, that doesn't mean the ePHI should be accessed for reasons not permitted by the Rule. In this particular instance, the system activity review report may need to be reviewed in conjunction with registration and scheduling data.

How do you know which employees or patients to review?

Individuals responsible for researching and responding to concerns and hotline calls—which stand to benefit from system activity review reports—must make use of appropriate system activity review reports. With regard to conducting proactive, regular reviews involving patients and employees, covered entities are strongly encouraged to use software that generates a random sample.

In addition, to make it easier to identify employees who may require additional attention, software rules should be put in place to generate reports when certain criteria are met, such as a physician viewing their spouse's ePHI, an employee viewing or sorting ePHI in search of desirable attributes for dating purposes, and employees viewing a coworker's ePHI.

How often should these reviews be completed?

Account access and activity reports cannot just be generated and reviewed in response to a concern or hotline call. The Rule specifically states that covered entities must implement procedures to *regularly* review system activity.

Unfortunately, this is a case where one size doesn't fit all. Covered entities will need to determine how often the regular reviews should

occur at their organization. In establishing this time period, the frequency of related hotline calls, investigations, and results of software-embedded rules, and such must be considered.

The Rule states that documentation such as system activity reviews must be retained for 6 years from the date of creation. Policies and procedures must be retained for 6 years from the date of creation or the date when it was last in effect, whichever is later.[3]

How do I know where to begin?

To get an accurate reading as to where your organization is in this process, a mock internal security audit may be helpful. If weaknesses and gaps are identified, implement remedial action.

Summary

Not all ePHI breaches may be prevented, but the use of system activity reviews may significantly reduce breaches caused by those inside the organization. Furthermore, system activity reviews are a starting place. Addressing outcomes of regular system activity reviews is a subject for a future article.

1. 45 CFR §164.308 (a)(1)(ii)(D)
2. 45 CFR § 312 (b)
3. 45 CFR§ 164.316

by Julie Hamilton, MBA, CHC; Yesenia Contreras, MHA, CPC, CPC-I; and Mark Schneider, MBA, CHC, CHRC

Effective compliance education: Moving from employee compliance to commitment

» The goal is to have more than just a "compliant" workforce; aim for a culture of commitment.
» Education is a tool in building a more committed workforce.
» Compliance training topics should be timely, relevant, and prioritized.
» Managers play a pivotal role in compliance education and dissemination.
» Learning can be a motivating tool to keeping employees engaged.

Julie Hamilton *(Julie.Hamilton@ynhh.org) is Vice President, Chief Compliance and Privacy Officer;* ***Yesenia Contreras*** *(Yesenia.Contreras@ynhh.org) is Compliance and Privacy Officer, System Initiatives; and* ***Mark Schneider*** *(Mark.Schneider@ynhh.org) is Compliance Educator/Specialist; all at Yale New Haven Health System.*

We in Compliance may be able to get employees to "comply" for a period of time, but will it lead to a long-term culture of commitment from our employees? In other words, how can we, the compliance team, inspire our employees to *want* to do what is right?

Our Compliance department included Professor Victor Vroom from the Yale School of Management at our mid-year planning meeting. We pondered the classic question that Victor posed—"Does the organization strive for only a compliant workforce, or does it endeavor to foster a culture where employees went beyond and were committed to doing right?"

One piece of this puzzle might lie with effective compliance education. This article will focus on some best practices in compliance learning to help better engage a committed workforce.

Just about everything we work on involves education; it is a primary driver of what we do. It is difficult to think of any compliance initiative that does not have learning as a main component (see Figure 1).

When we onboard new physician practices, one focus is on ensuring revenue integrity. Our compliance program uses a blended approach to compliance training. We sometimes need to be creative in approaching physician education. Clinicians often have unique needs and diverse work schedules; we try

Figure 1: Sample of education topics in compliance initiatives

Hamilton

Contreras

Schneider

to find ways to present the learning in ways that engage clinicians and maximize their time. For example, consider grand rounds presentations/continuing medical education, onsite coaching at physician practices, mobile learning, or adding a compliance education component to an existing practice meeting.

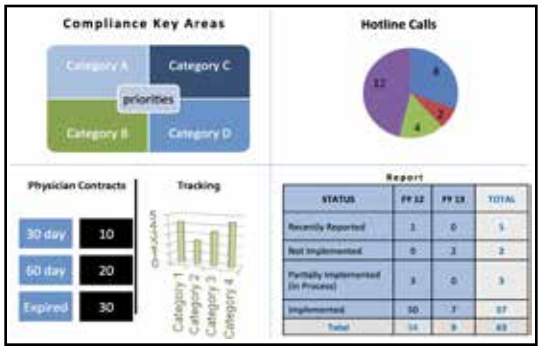


Figure 2: Example of a committee dashboard

The education topics should be timely, relevant, and prioritized to the needs or issues that are most pressing for the audience. If we see a coding or billing area that requires more attention, we make that an action item. Even if the physicians and staff had prior training on that topic, we might go back and reinforce the message or provide job aids. Practices in turn often become more "committed" when they see the compliance team is making an effort to really educate them on their unique compliance issues.

Compliance training should be viewed with the mindset of going beyond a one-time training event. Education can be a daily activity entwined in our weekly employee rounding. Having employees be continually engaged is the key. "Every day is a training day, and every event is a training event." — James Pritchert.[1]

Keeping the training focused is important. An education curriculum for a large health system may be complex in its design and deployment, but the warning to compliance officers is not to make the education message itself overly complex. It is important to keep it simple for our audience. Employees regard regulations as complex. The more we can demystify the message the better, and keep it succinct where possible. For example, use three short bullets (or less) in emails. Dashboard reports (see Figure 2) are effective, especially for executives.

Being visible, non-threatening, and approachable in the organization is an asset in building trust and relating with employees. Compliance professionals need to be cognizant of their tone in communications. We should be careful not to be too strong in conveying information at a level of intensity or negativity that may not be warranted. Use the most effective style for the situation. Employees need to feel comfortable coming into chat with us. These conversations offer coaching and informal training opportunities that help move employees toward being more committed.

Implementing a training strategy with many diverse types of entities and learners can pose challenges (e.g., from a large academic medical center with thousands of employees, to a rural physician practice that spans many miles). Creating solutions to maximize reach of remote and disparate learners is important, as well as matching the learning to the topic and modality. If our learners feel the training is not accessible or not applicable, the ability to connect with them is reduced, which may lead to a reduced commitment to follow policies.

Figure 3: Example of a compliance education structure

Figure 3 is an example of how a health system might structure a training program.

For example, a customized online course could be used for basic education and supplemented with opportunities for live events such as new employee orientation training, games (e.g. Stump the Compliance Officer, HIPAARDY), webinars, department in-service training on special topics, outside guest speakers, town hall meetings, brown bag breakfasts, board dashboards, podcasts, manager workshops, simulations, etc.

Compliance professionals should be careful not to make compliance education just a check-the-box exercise. I think we can all relate to a clinician joining a new organization and having 20 online classes assigned and due in 20 days, and the employee just doing what they can to get through the information quickly. How much of it sticks?

Having the basic regulatory training is necessary for compliance. However, we can be thinking about how to expand on that—and offer opportunities for question-and-answer or review cases/examples to better engage the learner. For example, just-in-time training solutions (such as job aids), compliance case studies, and simulations are effective. We tend to recall stories or cases and be able to apply the lesson learned later.

With the advent of electronic medical records and increased patient awareness that personal information maybe more easily accessible, the amount of privacy concerns has spiked. We are all feeling the increase in privacy concerns and need for additional training for our staff. Sometimes an effective way to make an impact with our employees is to ensure that managers and directors are also helping us educate—and re-educate. Managers have a key role in being able to disseminate information to staff and are a front line of defense. These leaders are often integral to reinforcing the message and keeping employees more connected and committed.

Additional suggestions include:

- Survey participants on what type or learning (topic and modality) the learners both want and need.
- Consider different approaches/modalities of regulatory learning solutions based on different categories of learners (e.g., board members, physicians, nurses, allied health professionals, managers, etc.)
- Leverage technology where possible to automate and manage learning processes (e.g., conflict-of-interest education and disclosures, course development, training reports, assignments)
- Regulatory compliance education may require using a combined approach (e.g., internally developed, vendor provided, partnered/shared, university supported)
- Consider a phased approach to speed implementation of new learning technologies vs. trying to do it all at once (e.g., phase 1-pilot, phase 2-inpatient, phase 3-outpatient, etc.)
- Organizations are pressuring educators for classes to be more focused, short, and to the point; consider instructional design solutions that maximize learner time, but achieve the goal, such as online training with a subsequent live webinar component.
- Always be benchmarking, looking to improve your compliance education, and gaining insights from publications (e.g., articles in *Compliance Today* or other professional publications) and attending conferences, etc.

Conclusion

Having robust and flexible compliance education solutions is one element in building and maintaining a compliant workforce and culture of professional commitment without having to use a carrot-and-stick approach.

1. http://bit.ly/JPritchert

SILENT AUCTION

to benefit America's Fund

Mark your calendar and make plans to attend the America's Fund silent auction! The silent auction will be held April 19–20 at the Walt Disney World Swan & Dolphin Resort during the 2015 Compliance Institute® in Lake Buena Vista, Florida.

Proceeds from the silent auction will benefit America's Fund, a non-profit charity that provides resources and financial support to injured and critically ill members of the U.S. Armed Forces and their families.

Some of the great items available include the script for the movie *National Treasure*, signed by the film's director Jon Turteltaub and producer Jerry Bruckheimer.

We are still collecting items for the auction.

If you or your company would like to contribute to this worthwhile event, please contact Kortney Nordrum at kortney.nordrum@corporatecompliance.org or 952-405-7928.

Learn more about HCCA's Compliance Institute
WWW.COMPLIANCE-INSTITUTE.ORG

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

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)®

- Deborah M. Alexander
- Leizyl Anglo
- Ida Ashour
- Valerie K. Baldwin
- John A. Beattie
- Deborah Bevilaqua
- Kristy Birmingham
- Melissa Borrelli
- Paul A. Bretz
- Linda Carl
- J. Douglas Clark
- Sheri Cosby
- Brendamarie Curtis
- Kevin Dahl
- Yvonne M. Daniels
- Jennifer Davis
- Julie A. Dyar
- Paul D. Filice
- Antonio Galan
- Kimberly J. Greenwell Miller
- Cheri Hahn
- Jennifer L. Hannagan
- Lindsey Harr
- Matthew S. Heilman
- Lisa Henning
- Katrina Howard
- Karen Hsu
- Sunmi Janicek
- Cheryl Jarman
- Katie M. Jedynak
- Lisa M. Lauer
- Rachel Liberatore
- Ellen N. Light
- Hector C. Lugo
- Kelly MacNeill-Cooney
- Maria Mantilla
- Luis F. Martinez
- Jon R. McMillan
- Monica S. Mejia
- Kellie Mendoza
- Jeremy Moser
- Dorothy H. Mukanjiri
- Jill Neale
- Neil R. Nokes
- Lauren Parsons
- Alberto L. Pena
- Freddy L. Perales
- Michele P. Randolph
- Annette A. Rangel
- Grace Rawlins
- Ronald R. Sagritalo
- Andrea Schock
- Varsha N. Shah
- Julie Sheehy
- Amy Simental
- Kari Snelson
- Ken A. Tasseff
- Christine J. Wilson
- Andrew Wintergerst

Certified in Healthcare Research Compliance (CHRC)®

- Aaron R. Alsleben
- Mark R. Schneider

Certified in Healthcare Privacy Compliance (CHPC)®

- Asra Ali
- Grant C. Garrard
- Erin M. Jack
- Tara L. McKibben
- Brenda L. Skorich

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

CHC™
Certified in Healthcare Compliance

Questions? Contact
ccb@compliancecertification.org

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.

COMPLIANCE CERTIFICATION BOARD®

HCCA *welcomes* NEW MEMBERS

ALABAMA
- Aaron Beam
- Amy Kerstetter, DST Health Solutions

ARIZONA
- Valerie Boerner, Banner Health
- Holly Dolgaard, Health Services Advisory Group
- Jane Johnson, Dignity Health

ARKANSAS
- Michelle Elliott, University of Arkansas for Medical Sciences
- Jenny Guthrie, Drew Memorial Hospital
- Mtonya Hunter-Lewis, University of Arkansas for Medical Sciences

CALIFORNIA
- Sabrina Butler, Sutter Health
- Christi-Ann Carlson, Santa Barbara Surgery Center
- Patti Carroll, Dignity Health
- Kulwinder Chhokar, Memorial Healthcare
- Betty DeLosReyes, San Francisco Health Plan
- Noeleen Farrell, Santa Rosa Community Health Centers
- Jacqueline Hanley, Kaiser Permanente
- Lisa Hatfield, United Indian Health Services
- Laura Hebert-Williams, Butte County Behavioral Health
- Eric Mah, University of California
- Rosalia McMillen, Davis Street Community Center Incorporated
- Justin Morrell, Adventist Health
- Mia Okinaga, Kaiser Permanente
- Tom Pattara, Children's Hospital of Orange County
- David Rigby, Sutter Health
- Anne Rohr, MedPOINT Management
- Scott Seaborn, County of Napa
- David Silva, PricewaterhouseCoopers
- Helen Soohoo, Kaiser Permanente

COLORADO
- Tisha Miller, Banner Health
- Lucia Padilla, Denver Health Hospital

CONNECTICUT
- Jaquel Patterson, Community Health Resources
- Rebecca Powell, Day Kimball Medical Group, Inc
- Ryan Taylor, RJ Health Systems

FLORIDA
- Terry Eden, Centrex Revenue Solutions
- Angela Forbes, Health First
- Nicole Griffin, Sunshine Health (Centene Corporation)
- Stephanie Hardman, Ludi, Inc
- Clayton Johnson, Florida Hospital
- Susan Kerrigan, Health First
- Thomas Meyers, Health First
- Alice Ventura, Florida Hospital

GEORGIA
- Kimberly Bryant, Wellstar Health System
- Glenda Stewart, NextStep Care

ILLINOIS
- Kristen Coates, Law Offices of Thomas J. Reed, Ltd
- Alicia Edens, Champians Fitness Physical Therapy
- Brenda Manning, R & B Solutions
- Dorothy Mukanjiri, Advocate Health Care
- Moses Suarez, SmithAmundsen, LLC
- Karas Zervos, Cook County Health & Hospital Systems

INDIANA
- Tony Akers, Williams Bros. Health Care Pharmacy
- Stanley Graber, Good Samaritan Hospital
- Sheree Tylicki, Franciscan St. Anthony Health
- Isaac M. Willett, Faegre Baker Daniels

IOWA
- Bridget Adams, University of Iowa Health Care
- Ron Boesch, Palmer College of Chiropractic
- Christina Gray, UnityPoint Health
- Melissa Ingrim, UnityPoint Health

KENTUCKY
- Lynn Bricking, Anthem, Inc
- Melissa Dant, Anthem, Inc

LOUISIANA
- Carey Hotard, Central Control, LLC
- Drew Williamsen, University Health
- Nicole Woody, University Health - Conway

MAINE
- Philip Jean, Harmony Healthcare International

MARYLAND
- Valerie Hayes, The ROI Companies
- Tanya Morgan, Technatomy Corporation
- Stephanie Shirey, Healthy Howard, Inc

MASSACHUSETTS
- Jared Barnes, Boston Medical Center
- Lydia Dollar, Baystate Medical Practices
- Kenna Jean-Baptiste, Tufts Health Plan
- Jason Rio, Health New England
- Eric Simoni, PricewaterhouseCoopers

MICHIGAN
- Stacy Coleman, LifeWays Community Mental Health
- Deanna Collison, McLaren Homecare Group
- Sue Levandoski, Spectrum Health
- Adrienne Savage, Blue Cross Blue Shield of Michigan

MINNESOTA
- Sheri Beck, Prime Therapeutics LLC
- Craig Downs, Prime Therapeutics LLC
- William Robinson, Target
- Joua Sobocinski, Center for Diagnostic Imaging

MISSOURI
- Larry Askew, Sizewise Rentals, LLC
- Sherry Hathaway, Liberty Hospital
- Aaron Henton, Cerner Corporation
- Denise Hill, Mercy Health System
- Melissa Jackson, Mercy Health System
- Kimberly Moran, HCCS Health Care Compliance Strategies
- Alicia Myles, Essence Healthcare
- Stephen Rothenberg, Centene Corporation
- Allison Trimble, Netsmart Technologies, Inc

NEBRASKA
- Mike Reisinger, CHI Health
- Eric Schram, Pharmaceutical Technologies, Inc

NEVADA
- Justin Dillman, Brian Citro MD PC

NEW HAMPSHIRE
- Jon DiGesu, Harmony Healthcare Inc

NEW JERSEY
- Maureen Cafferty, Springpoint Senior Living Inc
- Sudeep Chatterjee, Atlas Systems Inc
- Blake Freeman, Department of Veterans Affairs
- Gloria Gaines, Princeton University
- Leonora Hutchinson, Department of Veterans Affairs
- Sandi Ko, Springpoint Senior Living Inc
- Debra Lightner, Horizon Blue Cross Blue Shield of New Jersey
- Kerri McCutchin, Cooper University Healthcare

NEW MEXICO
- Andrea Kinsley, Presbyterian Healthcare Services
- Michelle Pacheco-Ortiz, Presbyterian Health Plan

NEW YORK
- Sandy Baxter, Canandaigua VA Medical Center
- Joseph DeMarzo
- Jackedja Francois, MetroPlus Health Plan
- Sami Manirath, Upper Allegheny Health System
- Matthew McGarvey, Harmony Healthcare International
- Sara Packman, New York City Department of Health

NORTH CAROLINA
- Sarah Crotts, Womble Carlyle Sandridge & Rice, LLP
- Tom Hines, A2Z Home Medical Supplies, Inc
- John Tillery, GW

OHIO
- David Fogarty, HealthSpan Partners
- Frank Giancola, CareSource
- Charles Hartig, Omnicare, Inc
- Wendy Henoch, Cleveland Clinic
- Tiffany Perrine, Nationwide Children's Hospital
- Lisa Trost, Envision Insurance Company
- Laura Wilson, Nationwide Children's Hospital

OKLAHOMA
- Peggy Warner, Mercy Health System

OREGON
- Janette Armstrong, Salem Health
- Leslie Conner, Avamere Health Services
- Kimberly Hanson, WVP Health Authority
- Manuel Rivera, WVP Health Authority

PENNSYLVANIA
- Patricia Hansrote, Deloitte & Touche, LLC
- Nicole Turner, Ernst & Young

RHODE ISLAND
- Marcy Olney, Neighborhood Health Plan of Rhode Island

TENNESSEE
- Tamara Huff, MediTract
- Hughes Johnson, Youth Villages
- Regan Tarpey, MediTract

TEXAS
- Kimberly Darwin-Scott, HPP
- Tuesdi Hill, City of Dallas
- Stephen Holloway, North Shore-LIJ Health System
- David Holtzman, CynergisTek, Inc
- Melissa Huff, Clinics of North Texas
- Jing Kainer, Houston Methodist Hospital
- Louise Lynch, Austin Travis County Integral Care
- Francis Mijares, Clinics of North Texas
- Dwane Moskwa, Kratos SecureInfo
- Cheryl Scott, Health Texas Provider Network
- Eric Scott, GroupOne Services
- Lindsay Taylor, Memorial Hermann
- Amber Weed, Community Health Choice

UTAH
- David Monaghan, Medical Billing Experts

VERMONT
- Patrick Mahoney, Central Vermont Medical Center

VIRGINIA
- Pamela Bennett, Department of Veterans Affairs
- Chris Bevil, Kratos SecureInfo
- Yong-Gon Chon, Kratos SecureInfo
- Per Segerstrom, Kratos SecureInfo

WASHINGTON
- Katherine Milts

WISCONSIN
- Bridget Krueger, iCAD Inc
- Terah Weidenhamer, Department of Veterans Affairs - CPAC

PUERTO RICO
- Gloria Amador Fernandez, Salud Integral en la Montana
- Florentino Aviles, Salud Integral en la Montana
- Edwin Bosques, Salud Integral en la Montana
- Clara Bou, First Healthcare Health System of Puerto Rico
- Carlos Gonzalez, G.H. Bass & Co
- Gerardo Hernandez, Salud Integral en la Montana
- Alberto Lopez, Salud Integral en la Montana
- Luis Martinez, Salud Integral en la Montana
- Mildred Morel Ortiz, Centro de Servicios Primarios de Salud de Patillas
- Eliu Moya-Ortiz, PryMed Medical Care, Inc
- Carola Pedraza, Medical Card System, Inc
- Liana Pomales-Cordero, Centro de Servicios Primarios de Salud de Patillas
- Ada Torres, Salud Integral en la Montana
- Anabelle Torres, Salud Integral en la Montana
- Angel Vega, Salud Integral en la Montana

PARAGUAY
- Andrea Campos-Cervera, Casa Boller S.A.

SAUDI ARABIA
- Hussameldin Selim, GlaxoSmithKline

JOIN HCCA
ON SOCIAL MEDIA

www.hcca-info.org

Takeaways

March 2015

Compliance TODAY

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

Fraud control strategy: Where to focus limited resources

Mia Okinaga (page 27)

- Focusing on the right initiatives will advance your fraud control program.
- Identifying anomalies and outliers will help create meaningful information for leadership.
- Enhancing data analytics tools allows for an organization to stay in front of regulators.
- Increasing the velocity of integrated learnings will create a stronger and leaner organization.
- Establishing an integrated staged fraud-control program will yield returns on investments.

Is your privacy monitoring up to snuff?

Nadia Fahim-Koster (page 31)

- Understand the requirements that drive the need for continuous logging and monitoring.
- Recognize the implications of the HIPAA Breach Notification Rule.
- Proactively position your organization to monitor risks of data breaches.
- Develop a monitoring program that is scalable to your organization.
- Learn how to develop a clear and accountable communication plan.

Compliance challenges in new chronic care management code

Peter A. Khoury (page 39)

- A new per-beneficiary-per-month chronic care management code will be available in 2015.
- The new code recognizes non–face-to-face services for patients who have chronic conditions.
- Evaluate clinical, technological, and compliance infrastructures before billing.
- Demonstrate and document the effectiveness of training about the code by conducting pre-session and post-session assessments.
- Conduct regular reviews early-on, and implement controls to monitor use.

340B drug program: Hospital audit readiness

Susan Prior and Cristine Vogel (page 43)

- Develop a comprehensive oversight and monitoring strategy to remain compliant within the complexities of the 340B program.
- Define clear policies and procedures for patient and prescriber eligibility.
- Review eligibility requirements and regularly update HRSA database.
- Incorporate frequent self-audits and annual external audit to ensure readiness.
- Develop community benefit plan to ensure HRSA's program intent.

Five tips for success in research compliance education

Emmelyn Kim and Tina Chuck (page 53)

- Create an organizational structure around education and training.
- Integrate all aspects of research compliance.
- Build partnerships, collaborate, and use a multi-disciplinary approach across departments.
- Use flexible adult learning methods in training programs.
- Continually evaluate your program with metrics for improvement.

Preventing and detecting fraud and abuse in a managed care network

Kim Keehn (page 57)

- Data mining is essential to detecting potential fraud and abuse in a network of providers.
- A cross-functional team using open communication is vital to the success of a compliance program.
- Implementing various program integrity strategies is the most effective way of eliminating fraud and abuse.
- It is important to have various means for reporting suspected fraud and abuse and providing education about those reporting methods.
- Reporting suspected fraud and abuse is the responsibility of everyone.

The Physician Payment Sunshine Act: Lessons learned in the first year

Jillian A. Watts (page 61)

- Registration for the Sunshine Act began July 14, 2014 for physicians and teaching hospitals.
- The registration process was frustrating and time consuming.
- The dispute resolution process was difficult to navigate.
- Data became publicly available on September 30, 2014.
- The data available did not paint a complete picture.

The talisman to ward off worthless services cases

Pamela Duncan (page 65)

- Worthless services cases generally stem from prolonged, substandard conditions.
- Defending a worthless services case is complicated, expensive, and arduous.
- Vibrant quality assurance committees help stave off worthless services claims.
- Effective quality assurance is comprehensive, collaborative, and improves outcomes.
- CMS-mandated quality assurance programs include five specific elements.

HIPAA Security Rule system activity reviews

Lisa I. Wojeck (page 69)

- The HIPAA Security Rule requires system activity reviews occur regularly.
- The HIPAA Security Rule requires covered entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems containing or using ePHI.
- Identify a leader to own the system activity review process.
- Accounting and audit configurations must be appropriately set to capture system events.
- System activity review reports must be reviewed in context with other pertinent data.

Effective compliance education: Moving from employee compliance to commitment

Julie Hamilton, Yesenia Contreras, and Mark Schneider (page 72)

- The goal is to have more than just a "compliant" workforce; aim for a culture of commitment.
- Education is a tool in building a more committed workforce.
- Compliance training topics should be timely, relevant, and prioritized.
- Managers play a pivotal role in compliance education and dissemination.
- Learning can be a motivating tool to keeping employees engaged.

HCCA's Upcoming Events

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

March 2015

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1	2	3 WEB CONFERENCE *Increase Your Value through HIPAA Education*	4	5 WEB CONFERENCE *Preparing Your Organization for Round Two: Tips for Surviving Privacy & Security Desk Audits*	6	7
	Healthcare Privacy Basic Compliance Academy San Diego, CA			CHPC Exam	**Regional Conference** St Louis, MO	
	Research Basic Compliance Academy San Diego, CA			CHRC Exam		
8 *Daylight Saving Time Begins*	9 **Basic Compliance Academy** Las Vegas, NV	10	11 WEB CONFERENCE *Patient and Data Privacy Considerations in a Private Health Information Exchange*	12 CHC Exam	13 **Regional Conference** Washington DC	14
15	16 WEB CONFERENCE *Settling False Claims Act Cases with the Federal Government*	17 *St. Patrick's Day*	18 WEB CONFERENCE *Medical Necessity Compliance and the Two-Midnight Rule*	19	20 **Regional Conference** Charleston, SC *First Day of Spring*	21
22	23	24	25	26	27	28
29 *Palm Sunday*	30 WEB CONFERENCE *Internal Compliance Surveys: Measuring Your Department's Effectiveness*	31	1	2	3	4

April 2015

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
29	30	31	1 *April Fool's Day*	2	3 *Passover Begins at Sundown Good Friday*	4
5 *Easter*	6	7	8	9 WEB CONFERENCE *Breach Risk Assessments Using Real Examples*	10	11 *Passover Ends*
12	13	14	15	16	17	18
19 **19th Annual Compliance Institute** Lake Buena Vista, FL	20	21	22 CHC, CHPC, and CHRC Exams	23	24	25
26	27 WEB CONFERENCE *OCR HIPAA Audit Program 2015 and Beyond: What We Know So Far* **Basic Compliance Academy** Orlando, FL	28	29	30 **Regional Conference** San Juan, Puerto Rico CHC Exam	1	2

Dates and locations are subject to change.

19th Annual Compliance Institute
April 19–22 • Lake Buena Vista, FL

Research Compliance Conference
May 31–June 3 • Austin, TX

Clinical Practice Compliance Conference
October 11–13 • Philadelphia, PA

Healthcare Enforcement Compliance Institute
October 25–28 • Washington DC

Basic Compliance Academies
March 9–12 • Las Vegas, NV — **SOLD OUT**
April 27–30 • Orlando, FL — **LIMITED SEATS REMAIN**
June 8–11 • Scottsdale, AZ
August 10–13 • New York, NY
September 14–17 • Chicago, IL
Sep 28–Oct 1 • Scottsdale, AZ — **JUST ADDED**
October 19–22 • Las Vegas, NV
October 26–29 • Nashville, TN
November 16–19 • Orlando, FL
Nov 30–Dec 3 • San Diego, CA

Healthcare Privacy Basic Compliance Academies
March 2–5 • San Diego, CA — **SOLD OUT**
June 15–18 • Las Vegas, NV
November 2–5 • Orlando, FL

Research Basic Compliance Academies
March 2–5 • San Diego, CA
November 2–5 • Orlando, FL

Regional Conferences
March 6 • St Louis, MO
March 13 • Washington DC
March 20 • Charleston, SC
April 30–May 1 • San Juan, PR
May 8 • Columbus, OH
May 15 • New York, NY
June 5 • Philadelphia, PA
June 12 • Seattle, WA
June 19 • Santa Ana, CA
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

Corporate Compliance & Ethics Week

November 1–7, 2015

Join organizations worldwide in championing workplace compliance and ethics

hcca-info.org/CandEWeek

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

Companies across the world highlight the importance of compliance and ethics during Corporate Compliance & Ethics Week.

Join us!

Celebrate Corporate Compliance & Ethics week in your organization and show your workforce how important compliance and ethics are to you. Promote your compliance program and work to build an ethical, speak-up culture.

Build on your regular training and increase awareness with a Corporate Compliance & Ethics Week celebration. HCCA has created tools and products to help organizations like yours advance your compliance and ethics goals.

Visit **hcca-info.org/CandEWeek** to download the free Train-the-Trainer kit, listen to a free webcast, sample products and posters to spread the word—and then join the hundreds of organizations celebrating Corporate Compliance & Ethics Week!

Health Care Compliance Association's 19th Annual

COMPLIANCE INSTITUTE®

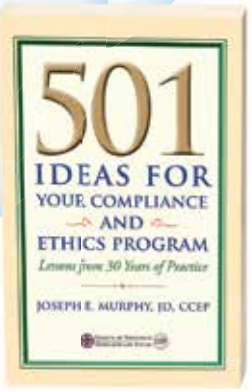
Lake Buena Vista, FL | April 19–22, 2015

Walt Disney World Swan and Dolphin Resort

Questions: jennifer.parrucci@hcca-info.org

SPECIAL OFFER

Register between March 1–31 and receive a free book (valued at $60)*



Plan now to take a CHC, CHPC, or CHRC certification exam at the Compliance Institute

All exams will be held Wednesday, April 22, 1:30–4:30 PM

Exam check-in: 1:00 PM

To download exam applications, visit compliance-institute.org and click the "Certification" tab. Exam applications should be mailed or faxed separately from the conference registration as directed on the exam application.

To be eligible to sit for an exam, candidates must acquire 20 CCB continuing education units, ten of which must come from "live" events or trainings. For a full list of exam requirements, please visit compliancecertification.org. One clock hour of session time at the Compliance Institute counts for 1.2 CCB CEUs. CCB CEUs are calculated on a 50-minute hour.

If you wish to receive credits for your attendance at this conference, you must complete and submit a Continuing Education Application (found inside the Conference Guide you will receive on-site at the Compliance Institute, or ask HCCA staff).

If you have questions, please email ccb@compliancecertification.org or call 888-580-8373.

CHC™ Certified in Healthcare Compliance

CHRC® Certified in Healthcare Research Compliance

CHPC® Certified in Healthcare Privacy Compliance

**Register for the 2015 Compliance Institute between March 1–31 and receive a free copy of* 501 Ideas for Your Compliance and Ethics Program: Lessons from 30 Years of Practice *(valued at $60). Offer good only for new registrations purchased March 1–31.*

LEARN MORE & REGISTER

compliance-institute.org

HCCA
HEALTH CARE COMPLIANCE ASSOCIATION