HCCA
hcca-info.org

Compliance TODAY

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

APRIL 2018

A smooth transition

an interview with
Gerry Zack
Incoming CEO
SCCE & HCCA

stress less, care more

Taking staff off the floor to complete mandatory compliance training is stressful. HCCS compliance training was developed with this in mind.

HCCS online compliance courses are interactive and mobile compatible, effectively engaging your staff while reducing seat time, so they can go back to what's most important—caring for your patients.

HIPAA Compliance

Professional Compliance

Corporate Compliance

Preventing Sexual Harassment

Stress less knowing you have an effective compliance training program.

hccs.com/StressLess

hccs
A HealthStream Company

by Gerry Zack, CCEP

At least I can remember my voice

Please don't hesitate to call me about anything any time.
952.567.6215 Direct
gerry.zack@corporatecompliance.org
@Gerry_Zack *in/gerryzack*

"Hey Siri, get directions to The Grill restaurant." "Hey Cortana, what's the balance in my checking account?" "Transfer $500 from savings to checking." "Pay $1,000 to American Express." "Provide access to my medical records with this healthcare provider." "Share my insurance information with this office."

At what point, if any, did those commands make you nervous? Voice recognition is rapidly replacing passwords and, if you believe the experts, is far more secure. Unlike a password, which might have 8 or 10 or 12 characters, voice identification software can analyze more than 100 behavioral and physical characteristics that are unique to each of us.

Zack

Banks have been recording our voiceprints to improve security for several years, and some now offer voice recognition alternatives to passwords for certain types of banking transactions, like account balance inquiries and intrabank transfers. However, it is estimated that by 2022, 31% of us will be making payments to third parties using voice recognition in place of passwords. And extending voice recognition to other areas that require security is inevitable. But it makes me a little nervous.

Yet, every time I get nervous about embracing new technology, I remind myself of the words of the German physicist, Max Planck, who won a Nobel Prize in 1918: "A scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents eventually die and a new generation grows up that is familiar with it."

So, adopting new technology seems to beat the alternative of holding on to something that is destined to be replaced. Voice recognition as security is here, like it or not. Dual factor authentication, like knowing a password and having a token, card, or chip, has improved security significantly, but still leaves vulnerabilities — vulnerabilities that can be further reduced through the use of biometrics, like voice recognition, fingerprints, etc.

...it is estimated that by 2022, 31% of us will be making payments to third parties using voice recognition in place of passwords.

But what if there's a breach? *NBC News* reports that 22 million people have had their biometric data stolen. And here's where I get worried. Unlike a hacked password, which can quickly be replaced, each of us has only one voice. Replacing our voices, fingers, or eyes after a breach just sounds like something I don't want to have to go through.

4th Annual

Healthcare Enforcement Compliance Conference

November 4–7, 2018
Washington, DC

REGISTER BY SEPT 12 TO SAVE

Join the Health Care Compliance Association for the 4th Annual Healthcare Enforcement Compliance Conference. Gain practical advice in this one-of-a-kind forum for attorneys and compliance officers. Go beyond legal analysis and learn how to implement systems to stay within the law.

Want to become Certified in Healthcare Compliance (CHC)®? Apply to take the optional CHC exam on the last day of the conference.

View the preliminary agenda online now

hcca-info.org/hecc

Questions? jennifer.parrucci@corporatecompliance.org

HCCA

by Roy Snell, CHC, CCEP-F

I know you

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*

On occasion, I get an email or message on LinkedIn from someone who thanks me for something I have done. There are a lot of people who know me that I do not know. It can be unsettling. I feel unappreciative, unaware, unknowledgeable or "un" something. I just got one of these messages on LinkedIn today from Julie Rys-Sours. She said, "I know you don't know me but…" and went on to say something very nice. These messages often start out with, "You don't know me but…." I have something to tell Julie. Frankly I have something to tell all of you.


Snell

I know you. You are a compliance professional. You are pushing the rock every day. You provided education that prevented someone from making a mistake that would have gotten them fired. They and their family would have suffered had it not been for you. But they will never know it. You help create a culture in your organization that has prevented a problem that would have embarrassed the whole company in the press. But they will never know it. I know you.

While the rest of the country just figured out that harassment is a problem, you have been putting in policies, investigating, educating, and doing many other things to prevent all kinds of harassment for years. And oddly enough, although everyone's hair is now on fire about harassment, you have had to fight for every hour of education, every policy, every investigation, and gotten grief because you made sure people were disciplined when necessary. People don't always get you, but I know you.

> "I know you don't know me but…"

You are kind and generous. You share your ideas with your peers. You help others. You speak at conferences, write articles, or simply take a call from a peer who needs a little of your time. You are doing something about the problems. You are taking definitive action. You are in the right job, although occasionally you kind of wonder. You are well educated. You care. You are compassionate. You are ethical. You have integrity. You take your job seriously. You are passionate. You are making the world a better place. You get it. I know you.

I know all of you.

Contents

April 2018

FEATURES

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).

COLUMNS

DEPARTMENTS

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 20, ISSUE 4

EY Survey: Global companies still unprepared for GDPR compliance

On January 31, 2018, EY announced the results of their Global Forensic Data Analytics Survey 2018. And according to their survey press release, "Intensifying regulatory pressures are top of mind for business leaders, with 78% of respondents expressing increasing concern about data protection and data privacy compliance." Ernst & Young noted that this "is the third biennial EY Global Forensic Data Analytics Survey, which examined the responses of 745 executives from 19 countries and analyzed the legal, compliance and fraud risks global companies face and the use of forensic data analytics (FDA) to manage them.

"However, with less than four months to go until the General Data Protection Regulation (GDPR) comes into force on May 25, 2018, only 33% of respondents state that they have a plan in place to comply with the EU legislation. While the average response of those in Europe was more positive, with 60% indicating they have a compliance plan in place, there is still much more work to be done in other markets where significantly fewer companies indicated readiness for GDPR compliance including Africa and the Middle East (27%), the Americas (13%) and Asia-Pacific (12%).

"Andrew Gordon, EY Global Fraud Investigation & Dispute Services leader, says: 'The pace of regulatory change continues to accelerate and the introduction of data protection and data privacy laws, such as GDPR, are major compliance challenges for global organizations. But businesses that adopt FDA technologies can achieve significant advantages, benefitting from more effective risk management and increased business transparency across all of their operations.'"

Link to survey:
https://go.ey.com/2Guzlj3

Five breaches add up to millions in settlement costs

On February 1, 2018, Health and Human Services Office for Civil Rights announced, "Fresenius Medical Care North America (FMCNA) has agreed to pay $3.5 million to the U.S. Department of Health and Human Services Office for Civil Rights, and to adopt a comprehensive corrective action plan, in order to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules."

According to the government press release, "In addition to a $3.5 million monetary settlement, a corrective action plan requires the FMCNA covered entities to complete a risk analysis and risk management plan, revise policies and procedures on device and media controls as well as facility access controls, develop an encryption report, and educate its workforce on policies and procedures."

For OCR press release: *http://bit.ly/2ECtD7I*

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

Regulatory News

CMS proposes Medicare Advantage and Part D payment and policy updates to provide new benefits for enrollees, new protections to combat opioid crisis

In February, the Centers for Medicare and Medicaid Services announced in a press release, "proposed changes for the Medicare health and drug programs in 2019 that increase flexibility in Medicare Advantage that will allow more options and new benefits to Medicare beneficiaries, meeting their unique health needs and improving their quality of life. Furthermore, the proposal includes important new steps to ensure new patient-doctor-plan communication in combatting the opioid crisis.

"As a part of these changes, CMS is redefining health-related supplemental benefits to include services that increase health and improve quality of life, including coverage of non-skilled in-home supports, portable wheelchair ramps and other assistive devices and modifications when patients need them."

For More:
http://go.cms.gov/2oiWGSD

Updates from CMS include: Quality Payment Program: Patient-facing encounters resources

In February, CMS posted the following resources on the agency's 2018 Resources webpage:

Patient-facing Encounter Codes Fact Sheet: Defines patient-facing encounters and details the categories included in the patient-facing encounter codes list;

- Patient-facing Encounter Codes List: Code and description for each patient-facing encounter;
- Operational List of Care Episode and Patient Condition Codes Background: Context for the information presented in the Operational List of Care Episode and Patient Condition Codes document; and
- Operational List of Care Episode and Patient Condition Codes: Operational list of eight episode-based cost measures and their corresponding episode group trigger codes.
- For More Information visit:
- Quality Payment Program website at *https://qpp.cms.gov*
- Resource Library webpage at *http://go.cms.gov/2Aud2j2*
- Contact the QPP Service Center at *QPP@cms.hhs.gov* or 866.288.8292 (TTY: 877.715.6222)

New York doctor sentenced to 13 years in prison for multi-million dollar health care fraud

In February, Acting Assistant Attorney General John P. Cronan of the Justice Department's Criminal Division announced, "A New York surgeon who practiced at hospitals in Brooklyn and Long Island was sentenced today to 156 months in prison for his role in a scheme that involved the submission of millions of dollars in false and fraudulent claims to Medicare."

According to the government press release, "Syed Imran Ahmed M.D., 51, of Glen Head, New York, was sentenced by U.S. District Judge Dora L. Irizarry of the Eastern District of New York, who also ordered Ahmed to pay $7,266,008.95 in restitution, to forfeit $7,266,008.95, and to pay a $20,000 fine. Ahmed was convicted in July 2016 after an 11-day trial of one count of health care fraud, three counts of making false statements related to health care matters and two counts of money laundering."
For more: *http://bit.ly/2Gu2CzZ*

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

EARLY BIRD EXTENDED

REGISTER BY **APRIL 25** AND SAVE

Research Compliance Conference

June 3–6, 2018 | Austin, TX

Join the Health Care Compliance Association for the primary education and networking event for research compliance professionals. Increase the effectiveness of your compliance program, discuss emerging risks, share best practices, and build valuable relationships.

Want to become Certified in Healthcare Research Compliance (CHRC)®? Apply to take the optional CHRC exam on the last day of the conference.

TWO CONFERENCES FOR THE PRICE OF ONE

Complimentary access to SCCE's Higher Education Compliance Conference is included with your registration.

hcca-info.org/research

Questions? taci.tolzman@corporatecompliance.org

HCCA™

HCCA *conference news*

Research Compliance Conference

June 3–6, 2018
Austin, TX
www.hcca-info.org/research

The risks associated with the conduct of clinical research are extensive, and these issues have garnered the attention of government regulators and enforcers alike. The 2018 Research Compliance Conference is the one event of the year wherein research compliance professionals, attorneys, audit professionals, scientists, research administrators, and healthcare executives can learn about these issues from the top industry experts. Unlike other research events, the Research Compliance Conference provides not only substantive information about the hot topics in research today, but it also focusses on practical strategies for addressing research compliance risks.

The agenda for the 2018 conference has a variety of industry experts who will share their knowledge on a wide variety of topics. The General Sessions include Research Year in Review, presented by Lisa Murtha, Senior Managing Director, Ankura Consulting Group; Whistleblowers in the Research Setting, presented by Melissa Markey, Attorney at Hall, Render, Killian, Heath & Lyman, PLLC; Clinical Trial Agreements and Unintended Compliance Issues, presented by Ryan Meade, Director of Regulatory Compliance Studies, Loyola University Chicago School of Law.

Please attend the Research Compliance Conference so that you will be on top of research compliance issues for your organization/clients as well. We look forward to seeing you June 3–6, at the Hilton in Austin, TX.

Find the latest conference information online ▶ 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 | About Membership | Events

Number of website visits last month

248,903

HCCA's 2018 Compliance Institute

Whether you're attending or not able to make it this year, be sure to check out the Compliance Institute website: *www.compliance-institute.org*.

You can find session descriptions, speaker bios, and presentations for the upcoming sessions, or you can choose which ones to go to before you ever leave home. You can view the Silent Auction items, so you know which ones you will be bidding on. And you can get all signed up for your networking experiences. From mentoring to volunteering, the Compliance Institute offers so much for its attendees.

If you are not attending this year, you can still see which sessions interest you. The recorded sessions will be available for purchase after the conference. You can even earn non-live CEUs for listening to the recordings.

Video of the month

Can qualify of care and compliance conflict?

David Hoffman, the president of David Hoffman & Associates talks about how quality of care relates to compliance. See this and other videos on onboarding and staff training at: *bit.ly/ct-vtom-2018-04*

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

HCCA *social media news*

Contact Doug Stupca at 952.405.7900 or email him at doug.stupca@corporatecompliance.org with any questions about HCCA social media.

LinkedIn — *hcca-info.org/Linkedin*

Join us on LinkedIn—a business-oriented network with over 300 million active users. With more than 15,000 members, our LinkedIn group fosters dozens of new discussion posts every week. One recent highlight:

Facebook — *facebook.com/hcca*

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

Pinterest — *pinterest.com/theHCCA*

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

Twitter — *twitter.com/theHCCA*

Join 12,000+ others and follow HCCA for breaking news and insights! Here is one recent favorite tweet:

Find the latest HCCAnet® updates online ▶ hcca-info.org/HCCAnet

HCCA *The Compliance & Ethics Blog Highlights*

Contact Doug Stupca at 952.405.7900 or email him at doug.stupca@corporatecompliance.org with any questions about HCCA's Blog.

Should Compliance Officers be striving to work themselves out of a job?

by Elvis A. Angyiembe

Regional Compliance Officer & Corporate Counsel, Panasonic Avionics Corporation, Dubai

Rigorous enforcement of anti-corruption laws over the last decade (or so) has led to a blossoming career for compliance officers (lawyers and other professionals) who work to help companies stay out of trouble and avoid penalties.

With no end in sight regarding enforcement, it seems that compliance officers may continue to be in high demand. It is a great thing for people already in the field and for those hoping to join.

Angyiembe

The question is...

Should compliance officers actually be striving to work themselves out of a job in the interest of their companies by helping build a strong compliance culture where there is little need for a huge compliance department?

A compliance culture...

Companies that depend solely on written policies to show that they care about compliance are not seeing the full picture. What is needed is a strong compliance culture from top to bottom where employees understand they do not need policies and compliance officers to tell them what to do or not to do.

I'd say that in a company with such a strong compliance culture, there is no need for a huge compliance department. You would probably need a few people who constantly pressure test the system to find any bad apples; but no need for a huge compliance department.

We all know we live in an imperfect world where so long as we have human beings with blood flowing through their veins and their self-interest to protect, employees will look for ways to beat the system and engage in conduct that could violate laws.

The challenge...

That notwithstanding, compliance officers should challenge their in-house clients to work them out of a job. That would be at a point where employees completely understand that compliance is not just the responsibility of one department, but the responsibility of everyone. A point where everyone does the right thing, the first time and always. A point where the risk of violation of laws and policies is very minimal with no need for a huge compliance department.

The reinvention

Compliance officers that embrace this challenge shouldn't be scared even if they work themselves out of a job. They could then reinvent themselves into something else and use their skills to help the company in others ways.

I embrace the challenge.

For more compliance news and insights, visit The Compliance & Ethics Blog at complianceandethics.org, and don't forget to subscribe to the daily digest at bit.ly/SCCEBlogSubscribe

Find the latest The Compliance & Ethics Blog updates online ▶ complianceandethics.org
Don't forget to subcribe to the daily digest ▶ bit.ly/SCCEBlogSubscribe

▶ SC Health Company, formed by a partnership between Greenville Health System (GHS) and Palmetto Health, has named **Joseph (Joe) J. Blake Jr.** as its Chief Governance Officer (CGO).

▶ **Michael D. Bossenbroek** has been named Senior Associate General Counsel at Beaumont Health in Troy, MI.

▶ **Sabrina DeLong** has been named Compliance Officer for the Vista School/Vista Foundation in Hershey, PA.

▶ Broward Health, Fort Lauderdale, FL, has announced the promotion of **Nicholas Hartfield** to the position of Vice President, Chief Compliance and Privacy Officer.

▶ **James Mathis** has been named UW Medicine's new Chief Compliance Officer in Seattle, WA.

PEOPLE on the MOVE

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*

Authors Can Earn CEUs:

CCB awards 2 CEUs to authors of articles published in *Compliance Today*

Compliance Today needs you!

Every month *Compliance Today* offers healthcare compliance professionals information on a wide variety of enforcement, regulatory, legal, and compliance program development and management issues.

We are particularly interested in articles covering compliance concerns involving hospitals, outpatient services, behavioral health, rehab, physician practices, long-term care/homecare/hospice, ambulatory surgery centers, and more.

Email your topic ideas and questions to *CT* News and Story Editor Margaret Dragon:
margaret.dragon@corporatecompliance.org

Gerry Zack, CCEP, CFE, CIA
Incoming CEO
SCCE & HCCA
Minneapolis, MN

an interview by Adam Turteltaub

Meet Gerry Zack

Gerry Zack *(gerry.zack@corporatecompliance.org) is Incoming CEO of SCCE & HCCA in Minneapolis, MN. He was interviewed in January 2018 by Adam Turteltaub (adam.turteltaub@corporatecompliance.org), Vice President, Strategic Initiatives and International Programs at SCCE & HCCA, based in Minneapolis, MN.*

AT: Gerry, welcome aboard. We're all excited about having you as the Incoming CEO, and I know there are a lot of questions people have about your background, what you'll be doing over the next year, and how the transition will work. I think the first thing people are going to want to know about is your career and what led you to us. Briefly can you walk us through what you were doing before you joined the association?

GZ: Thanks. I've been involved in compliance in one form or another virtually my entire career, even from the very beginning when I started out as an auditor. I was mainly doing compliance auditing, along with financial auditing and auditing government contractors, financial institutions, and organizations that got federal funding. So it was very heavy on compliance. I really had a taste for compliance from the get-go. That, ultimately, led to more of an investigative career.

I was trained as an accountant and was in forensic accounting doing investigative work, fraud investigations, regulatory compliance investigations, corruption investigations, things of that nature. That's where I really began working with Compliance departments and compliance functions within large

organizations and began learning how they really operated. It was through that angle that I dove head-long into the Compliance field.

I had my own forensic accounting and investigative practice for a number of years. I eventually got into the more proactive sides of compliance and fraud in terms of doing risk assessments, awareness and training programs, and things of that nature.

Most recently, I was with BDO in their global forensics group. The nice thing about that is it exposed me to the larger global organizations that I had limited exposure to when I had my own boutique practice.

AT: It must have been quite the broadening experience. I think it's interesting that you started in investigations, and so many compliance professionals struggle with the internal investigations part of the job. It's great that you have that experience. You mentioned that you spent a lot of time working in audit firms. Audit and Compliance tend to work very close together, as you well know. Do you see opportunities for them to work even closer together?

GZ: I think so. In fact, one of the more common weaknesses I saw when working with these larger organizations is a gap between Audit and Compliance, where Compliance wasn't doing what it really could be doing from a monitoring perspective, yet the missing pieces didn't fall neatly within what Internal Audit was doing, or Audit didn't have the knowledge or awareness to do that work.

AT: That was a really fun opportunity that sort of came out of the blue. It was great to spend a couple of years working with them. I oversaw their compliance function as well as being deputy executive director.

For starters, they are not opticians. These are people who study optics. They are scientists and engineers who are focused on the science of light. So, optics and photonics, everything from laser technology to all sorts of things I can barely pronounce. Working with them was fantastic. It's a global, growing organization that has a very diverse kind of a membership.

Being deputy executive director exposed me to the detailed inner workings of all aspects of a global, complex membership organization. I got to see a lot of things that the organization was going through. Up until then I had always been a third party, the consultant, the outside party that is brought in. The opportunity with the Optical Society gave me a chance to dive into the weeds of how a global membership organization functions.

AT: I have to say that I like the fact that both The Optical Society and the Society of Corporate Compliance and Ethics & Health Care Compliance Association (SCCE & HCCA) are about shedding light onto various issues. There's great similarity there.

You also spent time with the Association of Certified Fraud Examiners (ACFE), serving as a member of their board of regents and being a part of the faculty for their equivalent to our Academies. What were some of the lessons you learned from that experience that you'll be bringing over here?

GZ: The ACFE is about as close of a parallel to this organization as it gets. The similarities begin with an expanding definition of a profession. For the ACFE, it started out very narrow and began to broaden, just like we're seeing here, going from folks who perhaps had a very narrow interest in Compliance and a legal background, and now we have people joining from Risk Management or Internal Audit, and other fields as well, and that's where we're seeing many future opportunities for SCCE & HCCA.

SCCE & HCCA have additional parallels with ACFE in terms of its certification and

global growth. When you think of it, ACFE has about a 10-year head start on us. So, we can learn and perhaps mirror some of the things that they do.

My work with the ACFE also provided me with more firsthand observations and knowledge of how global growth in this type of a membership organization can be managed, as well as how its education and certification programs work, and I can bring that knowledge to the SCCE & HCCA.

AT: There's certainly a lot there, and I think it is notable how many people seem to go from fraud work to compliance and back and forth. As you know, we exhibit at ACFE conferences, and they exhibit at ours, and the overlap of people is just enormous.

Now that we have a sense of your professional background, what about you personally? What do you like doing outside of work?

GZ: My wife and I share a passion for international travel, exploring cultures, and hiking. One of our most exciting trips was in 2017 when we hiked in the Peruvian Andes at an elevation of 17,000 feet. For five days and four nights we were accompanied only by a Peruvian guide, a few local Quechua people, and a team of llamas. It was a physically demanding trek, but personally and culturally rewarding in so many ways.

AT: That does sound rewarding. Let's move now to how you came to know SCCE & HCCA and join us. You've been a member of SCCE for quite some time and even attended an Academy several years ago. I imagine you heard about the CEO opening from one of the emails that went out about it. What made you decide to pursue this opportunity after a career in Audit?

GZ: A number of things. One is my passion for the mission associated with compliance. I share the passion that the members have. This position also combines a lot of things in my background in terms of experience with associations, compliance, and even an entrepreneurial element. It hit all the right attributes, and I felt that I was a good match for the position. It also hit all the hot buttons for things that I really like to do. And, perhaps the final part of it really was that it was very clear that SCCE & HCCA had developed a sound transition plan. This wasn't a panicked search for a CEO by an organization that was in trouble.

AT: What were some of the other strengths you saw?

GZ: The organization is very much on an upward arc. Membership is growing, programs are doing well. It's both financially and operationally very stable. It's got a great staff, a great team here in Minnesota. It has a fantastic board of directors and Academy faculty. There are so many positives here, and really no negatives.

AT: I found when I switched jobs in the past that the interview process is a bit of a dance. You find out what you like about them. They, obviously, find out what they like about you. As you went through the process, was there anything that stuck out and made you think, "Wow, I didn't know this was there."

GZ: You know, it's interesting because one of the things that made things go so smoothly is that when I met with members of the search committee and others in the organization, it always just felt like a good conversation about the profession, its current state and its future, and where this organization is positioned to serve its members, to take advantage of opportunities and do great things for the profession.

There weren't any moments in the interview process in which some astonishing new insight came in. It was a nice gradual progression of getting to know the organization and having great conversations with everybody about the profession.

AT: Now that you've accepted the position and it's been announced, what are people from outside the organization telling you about us?

GZ: I've heard nothing but great things. Every message that I've received has been one of, "You've made a good decision." Hopefully, they think the organization made a good decision too.

This is a highly, highly respected organization. Virtually everybody who has touched SCCE & HCCA has come away with nothing but positive things to say. It's reinforced everything that I had learned about the organization up until that point.

AT: Let's move on now to the transition. November 1, 2017, was your official start as Incoming CEO. What will be the official date of your start as the actual CEO?

GZ: That won't happen until March of 2019. The transition plan that the committee and Roy came up with is a very solid one that enables me to gradually assume the role. That way, when Roy and I make that transition, I'll be fully up to speed and ready to assume the role of CEO.

AT: And obviously the goal there was to make it pretty seamless. It's an odd thing that it's a big change that you want to be as unnoticeable as possible. It's a long time between now and then. Can you talk to us about how the transition is going to work?

GZ: Our plan for these first few months is for me to basically learn the inner, operational workings of things here in Minnesota. I'm still learning who does what. But beginning early in 2018, I'll be shifting quite a bit, and my focus will be to get out, hit the road, and meet the members, because in the end, this is about listening to and serving the members. So, I want to meet as many people as possible. Count on me being at a lot of our events.

AT: Have you and Roy identified areas for you to focus on first for you to start getting your imprint on?

GZ: It's interesting because we're not really picking specific functional areas to assign as of a particular date. It's more of a gradual assimilation into the range of things that go into being a CEO.

There are a couple of exceptions to that, mainly because of timing. For example, we're going through the annual budgeting process right now (late 2017). What a great way to learn the organization. So, I'm diving into the budgeting aspect more than might be expected from an incoming CEO. Beyond that, though, we don't have a set schedule of specific functions on particular dates. It's more of a gradual learning and involvement in all the different functions of being a CEO.

AT: Well, there's certainly a lot there, as you've already seen. After Roy officially retires, he's still going to be around for a while. I understand he wants to do some writing. What else will his role be?

GZ: At a minimum, the writing piece. Roy is great at that. Let's face it. This is Roy Snell. I'll take any involvement I can get from Roy. To me it's a benefit. The longer Roy stays involved, the better, as far as I'm concerned. We haven't identified what the role will be. I think that will naturally develop based on what Roy's interests are and how much time he has to devote to the organization.

AT: And, mostly he'll be there to be a resource to you, as I understand it.

GZ: Absolutely, I'll be turning to Roy just as long as Roy will let me turn to him for insight and wisdom.

AT: I'm glad this transition has been mapped out. It's useful for the members and the staff knowing how smoothly this should transpire and that there won't be an abrupt shift of direction.

GZ: This is a great benefit for the organization and the membership to have this nice, lengthy transition. So many organizations miss this and have a one-month overlap between CEOs. I'm sorry, but you need more time, and the way this organization has mapped this out enables us to do that.

AT: It's terrific that it's working this way and you'll have that time over the weeks and months to come to get out and meet the members. Thanks for taking the time to do this interview, and thanks again for joining us.

GZ: Thanks. I'm thrilled to be here.

by Catherine Boerner, JD, CHC

Things are not always as they seem

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

This is truly an "Exhale" topic, because I really do believe most compliance and even some privacy issues are not as bad as they seem when first reported. Everyone really should exhale, stay calm, and just start the process of collecting the facts. Easier said than done, I know. Compliance officers and privacy officers don't know from one day to another what their day will be like and what concerns will be reported. It can be difficult sometimes to just stay calm emotionally and work the concern through to resolution. The ups and downs of the investigations can make you wonder where it will end up, but oftentimes, at the end of the day, things are not as bad as they may have seemed at first. That is why you cannot jump to conclusions.

Boerner

For example, you may have received a report and were told that a mom has called, alleging her son was kidnapped, and the kidnapper is breaching privacy by trying to get medical information about her son. (I know you think I am kidding, but I am not). After some fact finding, the real situation is that the ex-husband's new wife is trying to get her stepson's vaccine information to give to the new school. Mom is obviously not happy about it. (See…not so bad in the end.) We have to keep in mind that an individual's perception of events may not be factually accurate or communicated in the best way. Family dynamics and/or stress from a family member's illness and treatment clearly do contribute to the way compliance and privacy concerns may be reported.

> We have to keep in mind that an individual's perception of events may not be factually accurate or communicated in the best way.

I think this leads to insights into the best traits for a compliance officer and privacy officer to have. I think to best serve the organization, you need to be level-headed, have common sense, be willing to teach, and have a high emotional intelligence quotient (EQ). The dictionary defines EQ as "a measure of a person's adequacy in such areas as self-awareness, empathy, and dealing sensitively with other people." Most compliance and privacy concerns involve an inquiry to collect the facts, and that process can be intimidating and uncomfortable for many people involved. Therefore, having a strong self-awareness and capacity to recognize your own emotions and those of others will go a long way to being successful and recognizing things are not always as they seem.

CLINICAL PRACTICE COMPLIANCE CONFERENCE

Register by **August 14** to **SAVE $300**

(savings includes free pre-conference)

October 7–9, 2018 | San Diego, CA

The Health Care Compliance Association's **Clinical Practice Compliance Conference** enables you to build your network and gain the latest insights into best practices for compliance in a clinical setting. Get updated on government initiatives specific to physicians and their practice, and learn the latest enforcement trends.

Learn more at **hcca-info.org/clinical**

QUESTIONS? catherine.stollenwerk@corporatecompliance.org

HCCA™

by Andrew B. Wachler and Erin Diesel Roumayah

New resolution opportunities in the Medicare appeals process

- The Office of Medicare Hearings and Appeals' (OMHA's) appeal backlog continues to burden the appeals process and healthcare providers and suppliers.
- OMHA and CMS have demonstrated commitment to alleviating the backlog through releasing new and revised alternative dispute resolution (ADR) processes.
- The Low Volume Appeals (LVA) settlement and expanded Settlement Conference Facilitation (SCF) program collectively cover nearly every appeal under $100,000 that was pending with the Administrative Law Judge (ALJ) or Council levels as of November 3, 2017.
- The expanded SCF program, in conjunction with the LVA settlement, has the potential to collectively resolve a large volume of the appeals backlog.
- Medicare-participating healthcare providers and suppliers should continue to expect updates and expansions to existing ADR programs and the release of new programs until the backlog's growth has plateaued and/or the backlog is resolved.

Andrew B. Wachler *(awachler@wachler.com) is the Managing Partner and* ***Erin Diesel Roumayah*** *(eroumayah@wachler.com) is an Associate Attorney with Wachler & Associates, PC in Royal Oak, MI.*

Congress designed Medicare's administrative appeals process as an expedited resolution process for denied Medicare reimbursement claims. In fact, the Social Security Act prescribes specific timeframes within which Medicare appeals must be decided at each level of the administrative appeals process.[1] At the third level of the appeals process, which involves a hearing before an Administrative Law Judge (ALJ), Medicare appeals must be heard and decided within 90 days of a receipt of a request for hearing. According to statistics released by the Office of Medicare Hearings and Appeals (OMHA), the division of the U.S. Department of Health and Human Services (HHS) that administers ALJ hearings, beginning in 2008, OMHA began to receive more ALJ appeals than it could process, creating a backlog in the appeals process. In 2009, OMHA's average appeal processing time was 94.9 days, largely complying with federal mandate. That figure has steadily risen each consecutive year, and in 2017, OMHA's average appeal processing time exceeded 1,057 days.[2]

Wachler

Roumayah

The excessive adjudication delay has taken a significant financial toll on the Medicare provider and supplier community. The American Hospital Association (AHA) estimated that the value of Recovery Audit Contractor (RAC) appealed claims exceeded $1.8 billion. This figure does not include the value of non-RAC appealed

claims, which are also caught in the appeals backlog.[3]

Medicare providers and suppliers have called upon HHS, Congress, and the Courts to fashion remedies to the backlogged appeals process. The Audit & Appeals Fairness, Integrity, and Reforms in Medicare Act of 2015 (AFIRM) (S.2368) was introduced in the Senate and placed on the Senate legislative calendar on December 8, 2015. AFIRM proposed several reforms to the Medicare audit process, and although Congress has taken no action on AFIRM in well over two years, HHS has implemented on its own accord various reforms to the Medicare appeals process that are discussed in greater detail below. Judicial relief has been similarly slow. In 2014 the AHA and other healthcare providers filed suit in federal court against HHS, seeking a court order that HHS clear the backlog and comply with the 90-day statutory timeframe for ALJ hearings. The case is currently pending on remand before the United States District Court for the District of Columbia to evaluate HHS's claim that it is legally impossible to comply with a four-year resolution timetable as proposed by the AHA to reduce the backlog. According to this timetable, HHS would be required to reduce the backlog by 30% by 2018, 60% by 2019, 90% by 2020, and 100% by 2021.[4]

Congressional and judicial relief has been slow, but over the past years, HHS has released various initiatives to both reduce the backlog of pending appeals and curtail the filing of new appeals in the Medicare appeals process. These initiatives are welcome opportunities for Medicare providers and suppliers to achieve expedited resolution to pending appeals.

Low Volume Appeals settlement

On November 3, 2017, CMS announced a settlement opportunity for Medicare Part A and Part B providers and suppliers (appellants) with eligible fee-for-service appeals pending in the administrative appeals process. CMS titled this opportunity the Low Volume Appeals (LVA) settlement, because it allows appellants with less than 500 appeals pending before the ALJ or Medicare Appeals Council (the Council) levels of review, combined, to withdraw pending, eligible appeals from the backlogged Medicare appeals process in exchange for a non-negotiable settlement sum as final resolution of the disputed appeals. Through the LVA settlement, appellants will receive 62% of the net Medicare approved amount of their eligible claims.

Through the LVA settlement, appellants will receive 62% of the net Medicare approved amount of their eligible claims.

The LVA settlement is not the first settlement opportunity offered by CMS. In October of 2014 and November of 2016, CMS offered to pay eligible hospitals 68% and 66% of the net payable amount of their patient status claim denials in exchange for the hospital's acceptance of an administrative agreement as the full and final administrative and legal resolution of their claims. CMS defined patient status claims as claims denied on grounds that inpatient reimbursement for hospital services was not medically reasonable and necessary, but outpatient reimbursement would be appropriate. This settlement opportunity resolved approximately 346,000 claims from the backlogged Medicare appeals process. By August of 2016, CMS had executed settlements with 2,022 hospitals, amounting to nearly $1.47 billion dollars paid to participating hospitals.[5]

Although these settlements were attractive opportunities for eligible hospitals, large volumes of claims remained backlogged in the appeals process.

The LVA settlement has broader appellant eligibility criteria than the prior settlements. All Medicare Part A and Part B providers and suppliers are eligible, as long as they have less than 500 eligible appeals pending at the ALJ and Council levels of appeal, combined. Also, unlike the prior settlements, the LVA settlement contains no date of service restriction on eligible claims.

CMS provided the following appeal eligibility criteria for the LVA settlement:

- The appeal was pending before the OMHA and/or Council level of appeal as of November 3, 2017;
- The appeal has a total billed amount of $9,000 or less;
- The appeal was properly and timely filed at the OMHA or Council level as of November 3, 2017;
- The claims included in the appeal were denied by a Medicare contractor and remain in a fully denied status in the Medicare system;
- The claims included in the appeal were submitted for payment under Medicare Part A or Part B;
- The claims included in the appeal were not part of an extrapolation; and,
- As of the date the LVA settlement agreement is fully executed, the appeal was still pending at the OMHA or Council level of review.[6]

Appellants may be excluded from LVA settlement based on False Claims Act (FCA) litigation or investigation or other program integrity concerns, including pending civil, criminal, or administrative investigations. As with the other settlement opportunities, a participating appellant cannot choose to settle some eligible claims and not others. CMS has clarified that eligibility criteria are at the "appeal" rather than the "claim" level. This distinction is relevant, because the federal regulations permit appellants to batch or consolidate claims with similar issues of law and fact into one appeal for adjudication. Therefore, if the total billed value of the consolidated appeal exceeds the $9,000 cap, CMS would consider the appeal ineligible for LVA settlement, regardless of whether the individual claims have billed values well below the $9,000 cap. CMS has also suggested that if multiple claims were consolidated into one appeal and assigned one appeal number, those claims will be considered one appeal for purposes of the LVA settlement. For example, if a provider has consolidated for ALJ appeal 10 claims, each with a billed value of $1,000, and one ALJ appeal number has been issued regarding all 10 claims, OMHA would consider this as one appeal for purposes of LVA settlement. The billed value of the consolidated appeal would be $10,000, and these claims would be ineligible for the LVA settlement.

CMS created two separate participation periods for the LVA settlement to manage the volume of participants in the process and ensure timely processing of all requests. An appellant's National Provider Identifier (NPI) number will determine when it may request participation. To participate in the LVA settlement, an appellant should submit an Expression of Interest (EOI) form to CMS. For appellants with NPIs ending in an even number, EOIs will be accepted beginning on February 5, 2018 through March 9, 2018. If an NPI ends in an odd number, EOIs will be accepted beginning on March 12, 2018 through April 11, 2018. If an appellant has both an odd NPI and even NPI, it should submit an EOI for each NPI according to the timeframes above.

The LVA settlement is a fully voluntary process that allows an appellant to retain

full appeal rights until it signs the settlement agreement and submits it to CMS. However, once the settlement agreement is signed by the appellant and CMS, all claims identified as eligible on the final spreadsheet will be placed in a "pended" status with CMS and OMHA, and any proceedings on these claims will be stayed. If an appellant wishes to abandon the LVA process prior to execution of the settlement agreement, the appeals will remain in the normal appeals process and retain their place in queue for administrative resolution. Any specific appeals determined to be ineligible for settlement will return to their position in the appeals process.

Interested appellants should note that as of the date an appellant signs the settlement agreement, it will not know the exact net settlement value of the eligible appeals. Therefore, prior to signing the settlement agreement, appellants should prepare an educated estimate of their anticipated settlement payout under the LVA process.

Settlement Conference Facilitation Program

On November 3, 2017, CMS announced that in April 2018 it would be expanding its previously released Settlement Conference Facilitation (SCF) program to appellants not eligible for the LVA settlement. SCF is an alternative dispute resolution process that allows Medicare Part A and Part B healthcare providers and suppliers to negotiate a lump-sum settlement of eligible claims with CMS. SCF is fully voluntary, such that CMS or eligible appellants may refuse to participate in the program or withdraw from the program at any point prior to reaching settlement. If a settlement is reached, a settlement agreement is signed the day of the settlement conference, and the settled claims are withdrawn and dismissed from the ALJ hearing.

The voluntary and expedited nature of the SCF process has been attractive to Medicare appellants. If settlement is not reached, an appellant's claims return to the ALJ appeals process in the order in which they were originally received. Also, SCF offers an expedited resolution process compared to the ALJ appeals process. OMHA did not provide a firm start-to-end time table for completion of the SCF process, but it estimated a minimum of 10 weeks from the date an appellant receives OMHA's spreadsheet identifying eligible claims. In comparison to the Medicare appeals process that at recent estimates takes nearly 151 weeks at the ALJ level of appeal alone, SCF offers an expedited resolution process.

SCF was initially released in June 2014 for Medicare Part B providers and suppliers. For a Part B claim to be eligible, an ALJ hearing request had to have been filed in 2013, and the appeal could not already be assigned to an ALJ for hearing. In the fall of 2015, OMHA expanded SCF in a Phase II program for ALJ hearing requests filed on or before September 30, 2015, and not yet scheduled for ALJ hearing. Under Phase II, at least 20 claims must be at issue or at least $10,000 must be in controversy if fewer than 20 claims are involved.[7] OMHA estimated that the initial phase of SCF successfully settled more than 2,000 unassigned Medicare Part B ALJ appeals.[8]

In February 2016, OMHA expanded SCF to all Medicare Part A providers in a Phase III program. For a Part A claim to be eligible, the ALJ hearing request must have been filed on or before December 31, 2015 and not yet scheduled for ALJ hearing. Additionally, each individual claim must be $100,000 or less, and there must be at least 50 claims and $20,000 collectively in controversy. Additional eligibility criteria for the Phase III SCF process are located on CMS's website.[9]

CMS has published preliminary eligibility criteria for the new expanded SCF:

- The appellant must be a Medicare provider or supplier that has been assigned an NPI;
- The appeals involve request(s) for ALJ hearing or Council review filed on or before November 3, 2017, with a total of 500 or more appeals pending at OMHA and the Council combined; or with any number of appeals pending at OMHA and the Council that each have more than $9,000 in billed charges;
- The request(s) for ALJ hearing and/or Council review must arise from a Medicare Part A or Part B Qualified Independent Contractor (QIC) reconsideration decision;
- All jurisdictional requirements for OMHA or Council review were met for the eligible appeals;
- The amount of each individual claim in an appeal must be $100,000 or less (for the purposes of an extrapolated statistical sample, the overpayment amount extrapolated from the universe of claims must be $100,000 or less);
- The appellant cannot have filed for bankruptcy and/or expect to file for bankruptcy in the future; and
- Certain appellants will be ineligible if they have or have had FCA litigation or investigations pending against them, or other program integrity concerns, including pending civil, criminal, or administrative investigations.
- Additional eligibility limitations are explained on CMS's website.[10]

Statistical Sampling Initiative

Another alternative to the Medicare appeals process for Medicare appellants is OMHA's Statistical Sampling Initiative (SSI), announced in June 2017. The purpose of SSI is to efficiently resolve large volumes of pending ALJ appeals through the use of statistical sampling. More specifically, an ALJ hearing is conducted on a random sample of an appellant's pending and eligible ALJ appeals, and the ALJ's determination on those sampled claims is then statistically extrapolated to all of the appellant's pending and eligible claims.

SSI was previously released as a pilot project in late 2014. The pilot was fairly limited in scope, applying to claims that were assigned to one or more ALJs or filed between April 1, 2013, and June 30, 2013. Due to the structure of the pilot, many appellants were hesitant to participate. Specifically, only one ALJ hearing would be conducted on all of an appellant's eligible appeals, which rightfully gave most appellants pause, because favorable rulings on appeal range from 18% to 85% among ALJs.[11,12] For many appellants, participation in the SSI pilot was simply too risky. OMHA responded to these limitations of the pilot program in designing the SSI.

> OMHA estimated that the initial phase of SCF successfully settled more than 2,000 unassigned Medicare Part B ALJ appeals.

First, the new SSI contains no filing date restriction, which broadens the claim eligibility pool. SSI has broad claim eligibility requirements that are set forth on CMS's website.[13] Secondly, the new SSI employs a panel of ALJs. If a provider has 250 to 749 claims at issue, a random panel of three ALJs is assigned, and each ALJ will hear and decide one third of the sampled claims. If a provider has 750 claims or more, a random panel of four or five ALJs is assigned, and each ALJ will hear and decide one-fourth to one-fifth of the sampled claims. Although each ALJ on the panel will conduct its own hearing on its portion of the statistically sampled claims, the lead ALJ

will combine the decisions from each hearing on the sampled claims and issue one decision, which OMHA's statistical expert will extrapolate to the universe of claims.

An appellant can request statistical sampling, or OMHA can invite an appellant to participate in SSI. Once an appellant proactively expresses interest in the program or timely consents to OMHA's invitation, OMHA will generate a list of potential claims that make up the universe of eligible claims. The appellant has the opportunity to review the potential list for completeness. Thereafter, an ALJ will conduct a prehearing conference to discuss and finalize the universe of claims, review the proposed statistical sampling process, and answer any questions. Following the prehearing conference, the ALJ will issue a post-conference order, which will become binding within 10 calendar days of receipt if no objections are filed. Then, the sampled claims will be combined and assigned to a lead ALJ for hearing.

If an appellant timely withdraws its consent to SSI, the appeals will be returned to the standard ALJ hearing process. With broader eligibility criteria and the use of an adjudication panel, OMHA indicated on its website that, "[OMHA] hopes these changes make this program more attractive and that appellants actively consider participation in the program."

Conclusion

Medicare providers and suppliers with appeals pending in the Medicare appeals process have a variety of alternative dispute resolution processes to consider that were not available in years past. Eligible appellants should evaluate and consider participation in these processes, because they are likely to offer expedited and efficient resolution of large volumes of pending appeals in comparison to the backlogged appeals process. Also, these processes may offer a more favorable resolution than the standard appeals process, given recent trends in favorable rulings on appeals by ALJs. According to statistics released by the Government Accountability Office, appellants generally fare less favorably at ALJ hearing today than in years past. By way of example, the percentage of Part A Medicare fee for service appeals reversed by OMHA has steadily decreased since 2010.[14] In today's appeals climate, there is appreciable value to guaranteed settlement payouts and expedited resolution processes.

1. 42 U.S.C. § 1395ff (Determinations; appeals)
2. Office of Medicare Hearings and Appeals (OMHA) website at http://bit.ly/2C2AbLo
3. See American Hospital Association v. Burwell, 209 F. Supp. 3d 221 (D.D.C. September 19, 2016. Plaintiff's. Motion for Summary Judgement at 15). Available at http://bit.ly/2sDGp0m
4. See AHA v. Burwell, Case 1:14-cv-00851-JEB. December 5, 2016. Available at http://bit.ly/2ofl0oP
5. CMS.gov: Hospital Appeal Settlement Update. Available at http://go.cms.gov/2ExiVeE
6. CMS.gov: Low Volume Appeals Initiative. Available at http://go.cms.gov/2kBwOjV
7. OMHA: SCF Phase II eligibility criteria. Available at http://bit.ly/2qPp9ie
8. OMHA: SCF Phase III Appeal Eligibility. Available at http://bit.ly/2qPp9ie
9. Ibid, Ref #8
10. OMHA: Expanded Settlement Conference Facilitation. Available at http://bit.ly/2EwgIQN
11. HHS OIG: Improvements Are Needed at the Administrative Law Judge Level of Medicare Appeals, OEI-02-10-00340. November 2012. Available at http://bit.ly/2C1Dqm1
12. Judi Nudelman: Statement to the House Committee on Ways and Means, Subcommittee on Health, Current Hospital Issues in the Medicare Program, Hearing May 20, 2014. Available at http://bit.ly/2F6fywh
13. HHS.gov: Statistical Sampling Initiative Update. Available at http://bit.ly/2sw3K40
14. Government Accountability Office: Medicare Fee-For-Service: Opportunities Remain to Improve Appeals Process. GAO-16-366; May 10, 2016. Table 17 at Page 69. Available at http://bit.ly/2HlZEi4

by Lynda S. Hilliard, MBA, RN, CCEP, CHC

Taking a mental health day

Lynda S. Hilliard *(lyndahilliard@hotmail.com) is Principal of Hilliard Compliance Consulting in Mount Shasta, CA.*

There's too much going on! The pressures of work, family, personal commitments, and other stressors are weighing us all down. We had a nice break during the holidays, but that seems like months ago! What can we do to rejuvenate and revitalize our outlook and attitude on what we are trying to accomplish?

Well, in the old days, we took a "mental health" day—a day just to ourselves for resting, exercising, getting a massage, just being, or just breathing. We need to do that more often. We need to treat our mental health like we do our physical health. Negativity breeds more negativity and leads to less productive and creative work. A fresh outlook and renewed commitment to our goals, objectives, and passions is what is needed.

Hilliard

The gauge of mental health needs fluctuates between distraction and a lack of focus, to depression and inability to complete tasks. This column is too short (and written by a non-mental health professional) to deal with an individual who is in major need of a referral to a mental health professional. This is geared towards the "one-offs"—the people who need to refuel their psychic fuel sources periodically to keep moving in a positive direction.

On one end of the mental health spectrum, the federal Department of Health and Human Services recently estimated that only 17% of the U.S. population is functioning at optimal mental health; while at the other end, the Center for Prevention and Health estimates mental illness and substance abuse issues cost employers as much as $105 billion annually.[1] This issue is growing and needs to be addressed at all levels of a department or organization.

Several signs indicate we may need more time to reconnect with ourselves, and you might recognize a few:

- You get "set off" by little things.
- You are feeling down in the dumps.
- You are getting sick more than usual.
- You feel like you are moving in slow motion.
- You feel like you are distracted by something you need to do.
- You feel disconnected from your family and friends.

The above signs can help you recognize an impending need and alert you to act. Take a mental health day—*relax*, *reconnect*, *recharge*, and keep moving forward.

1. Amy Morin: "How to Know When to Take a Mental Health Day" *Psychology Today* blog; July 12, 2017. http://bit.ly/2uApE5U

Research *Basic Compliance* Academies

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.

Become Certified in Healthcare Research Compliance (CHRC)®

Apply to take the optional CHRC exam on the last day of the Academy

ONLY 1 MORE CHANCE IN 2018:

Orlando
December 3–6

hcca-info.org/academies

Questions? *taci.tolzman@corporatecompliance.org*

HCCA

Healthcare Privacy *Basic Compliance* Academies

HCCA's Healthcare Privacy Basic Compliance Academy® covers 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.

Become Certified in Healthcare Privacy Compliance (CHPC®)

Apply to take the optional CHPC exam on the last day of the Academy

Seattle
July 23–26

Nashville
October 15–18

Orlando
December 3–6

HCCA

hcca-info.org/academies

Questions? *catherine.stollenwerk@corporatecompliance.org*

by Lisa Knowles, RHIT, CCS

Passing the HCC Audit: What you need to know

» Diagnosis codes are based on the ICD-10-CM guidelines for the current fiscal year.
» Medical record documentation is key and must support the code assignment.
» Each face-to-face encounter must have a valid signature.
» A valid date of service must be on the documentation for each face-to-face encounter.
» Addendums are valid if based on an observation on the date of service.

Lisa Knowles *(lknowles@harmony.solutions) is a Compliance, Education and Privacy Officer at Harmony Healthcare in Tampa, FL.*

The Centers for Medicare & Medicaid Services (CMS) introduced Hierarchical Condition Categories (HCCs) and the architecture of the Risk Adjustment Factor with their mandate in 1997. The implementation of HCCs by CMS for the Medicare Advantage plans began in 2000, and they have been steadily phasing in this process over time. Since its inception, the understanding and significance of HCCs has grown and taken on considerable financial importance for physicians, physician groups (and physician extenders), health systems, and Medicare Advantage plans.

Knowles

CMS defines HCCs as a risk adjustment model used to calculate risk scores to predict future healthcare costs. It is a predictive model—based on medical record documentation and submitted ICD-10-CM diagnosis codes for the plan enrollees—with an underlying purpose to adjust capitated payments made to providers in these plans based on the beneficiaries' health. Of note, like any other CMS reimbursement methodology, the HCC Risk Adjustment Factor platform is subject to audit by CMS and its contractors.[1]

Tips for passing the audit

When thinking about data submission for the HCC Risk Adjustment Data Validation (RADV) audit, it's best to approach it in components. Here's what you need to know to successfully pass the audit.

Code to the guidelines

The majority of conditions submitted for HCCs are chronic conditions (a few acute conditions qualify as well) that the patient has, which have been documented by the provider with ICD-10-CM diagnosis code(s) submitted on the claim form. In the HCC system structure, patients are placed into categories based on the ICD-10-CM diagnosis code assignment; the ICD-10-CM code assignments group patients who are clinically similar into the same group (HCC). The structure is then further divided so that the groups break down into similar predictive costs for the beneficiaries' future healthcare costs. For consideration, there are more than 9,500 ICD-10-CM diagnosis codes that map to one or more of the 79 HCC codes in the CMS-HCC Risk Adjustment model. An ICD-10-CM code can map to more than

one HCC, because ICD-10-CM contains combination codes (i.e., a code can represent two diagnoses or a diagnosis with a complication).

At the foundation of HCCs is accurate coding of the ICD-10-CM diagnosis code based on the documentation found in the medical record. The following should be adhered to when coding:

- All ICD-10-CM coding assignments should be based on the *ICD-10-CM Official Guidelines for Coding and Reporting*[2] for the current fiscal year.
- Section IV of the guidelines has specific instructions for coding and reporting of outpatient services. Section I for conventions, general coding guidelines, and chapter-specific guidelines applies to the outpatient setting and professional fee coding for physician and non-physician provider services.
- Section IV of the guidelines requires that all documented conditions must be directly "relevant" to or "affect" the specific encounter. Providers are required to document all conditions evaluated during each face-to-face visit; this documentation should include the history of present illness (HPI), examination, and medical decision making.
- Per Section IV, subsection J:
  - Code all documented conditions that coexist at the time of the encounter/visit, and require or affect patient care, treatment, or management.
  - Do not code conditions that were previously treated and no longer exist. However, history codes (categories Z80–Z87) may be used as secondary codes if the historical condition or family history has an impact on current care or influences treatment.
- Per Section IV, subsection I, chronic diseases treated on an ongoing basis may be coded and reported as many times as the patient received treatment and care for the conditions.

Put MEAT in the documentation

The coding for HCCs is only as good as the documentation found in the medical record. As HCCs continue to evolve, best practices for documentation in the HCC world follow the culture of MEAT, which is an acronym that auditors have used to describe the four requirements for complete and accurate documentation:

- **Monitor**–the patient's signs, symptoms, disease progression, disease regression;
- **Evaluate**–test results, medication effectiveness, response to treatment;
- **Assess/Address**–ordering tests, discussion, review records, counseling; and
- **Treat**–medications, therapies, other modalities ordered by the provider

The MEAT acronym can be used as a valuable general guideline for physicians and auditors, but there is no "official" regulation to substantiate the use of this personnel guideline. As stated previously, always use guidelines and regulations published from official sources to ensure compliance.

A documentation area that continues to be problematic for providers is the Problem List. Simply making a list of diagnoses and adding them either in the electronic health record (EHR) or under the Assessment and Plan, without documenting in the face-to-face encounter that the patient's condition has been properly addressed during the visit and met the components of MEAT, is unacceptable (See Table 1).[3]

As noted in Table 1, the diagnoses on the problem list must have documentation that supports that all diagnoses listed were addressed and evaluated in the face-to-face encounter.

Table 1: CMS Contract-Level RADV Medical Record Reviewer Guidance

What the Reviewer May Encounter	Explanation/Examples	Reviewer Guidance	RADV Auditor Action
Problem Lists (within a medical record)	See related topic of Chronic and Other Additional Diagnoses. Lists of diagnoses (conditions, problems) may be numbered, bulleted, or separated by commas. A list may be documented in the patient history, assessment, discharge summary, or other areas of a medical record. When conditions commonly associated are listed under the same number or bullet, the conditions can assume to be linked. These diabetes examples are effective for ICD-9-CM and will be updated for ICD-10-CM. ***Example 1:*** 1. Hypertension 2. DM, neuropathy (link diabetes and neuropathy) ***Example 2:*** 1. Hypertension 2. DM 3. Neuropathy (do not link diabetes and neuropathy) ***Example 3:*** 1. Diabetes with hypertension) Although these conditions could occur together and berelated, unless the documentation clearly shows a cause and effect relationship, do not link diabetes and other condition if not typically a known manifestation of diabetes.)	Evaluate the problem list for evidence of whether the conditions are chronic or past and if they are consistent with the current encounter documentation (i.e., have they been changed or replaced by a related condition with different specificity). Evaluate conditions listed for chronicity and support in the full medical record, such as history, medications, and final assessment. Do not submit conditions from lists labeled as PERTINENT NEGATIVES.	Problem lists are evaluated on a case-bycase basis when the problem list is not clearly dated as part of the face to face encounter indicated on the coversheet or there are multiple dates of conditions both before and after the DOS. Lists of conditions written by the patient are not acceptable. Lists of code numbers without narratives are not acceptable. Mention or EMR population of diagnoses in a list will be considered on a caseby-case basis for RADV once all other coding rules and checks for consistency have been applied.

Valid signatures are a must

The physician/provider must include a valid signature for the dates of service submitted for review and audit on each encounter. This applies if the physician/provider is on an EHR and signs with an electronic signature or, if the records are submitted in paper format, the physician/provider must sign the actual paper record. Of note, CMS-generated attestations can be submitted for physician/practitioner and hospital outpatient medical records only. These must be completed, signed, and dated by the physician/practitioner who provided those services. No other forms of attestation will be accepted. The completed fields must include the printed physician/practitioner's name, the date of service on the medical record to which they are attesting, the physicians/practitioner's specialty or credential, and must be signed and dated by the physician/practitioner that conducted the face-to-face visit. If the encounter does not have a valid physician/provider signature, it is not considered a valid submission for audit.

Date of service is required

The date of service for the face-to-face encounter must be easily accessible and validated on the encounter. An encounter submitted without a date of service that can be validated is considered invalid and is unacceptable for audit.

Addendums/amendments to the medical record

Medical record addendums/amendments are accepted and considered valid documentation for audit if they are based on an observation of the patient made on the date of service/encounter by the attending physician. The most common form of addendum/amendment is based on a diagnostic test ordered on the date of service and the test results received following the patient's visit. The addendum/amendment must contain ample information to verify that it was completed in a timely manner; this timeframe generally means 90 days. Most facilities and practices have a 30-day time limit for the completion of addendum/amendments.

Summary

The above are the top five troublesome areas frequently encountered in HCC audits. In reviewing these and providing detail, we can focus on improving these areas with our physicians/providers, coders, outpatient clinical documentation integrity, and other team members to improve audit findings and accuracy scores. More importantly, it will ultimately reflect an accurate predictive healthcare cost for the Medicare beneficiary population.

The opinions expressed are those of the author and do not necessarily reflect the views, policies, or opinions of Harmony Healthcare.

1. CMS Online Manuals: Medicare Managed Care Manual, Chapter 7 – Risk Adjustment. Available at http://go.cms.gov/1Wy79H2
2. Centers for Medicare and Medicaid Services (CMS) and the National Center for Health Statistics (NCHS): ICD-10-CM Official Guidelines for Coding and Reporting FY 2018. Available at http://bit.ly/2uwSEbw
3. CMS: Contract-Level Risk Adjustment Data Validation, Medical Record Reviewer Guidance as of September 27, 2017. Available at http://go.cms.gov/2EoCnKB

by Nancy J. Beckley

Put it in your Pocket, save it for another day

Nancy J. Beckley *(nancy@nancybeckley.com) is President of Nancy Beckley & Associates LLC, a rehab compliance consulting firm in Milwaukee, WI.*
/in/nancybeckley *@nancybeckley* *+NancyBeckley*

In the "old" days, clippings from newspapers, magazines, and brochures joined cards and pictures that were stored safely in desk drawers, file cabinets, and bedside tables, all ready for when there was time to read, be inspired, or simply to look back and reflect. In the inevitable New Year's "tidy up" resolutions earlier this year, I worked through the collection. A professional organizer would be proud!


Beckley

And then it was on to my "Pocket"—electronic clippings of digital articles that I had been collecting for the past several years. Pocket is undoubtedly my favorite app. Take a peek at *getpocket.com*, where they remind you, "When you find something you want to view later, put it in Pocket. Save for later: Put articles, videos or pretty much anything into Pocket. View when ready: If it's in Pocket, it's on your phone, tablet or computer. You don't even need an Internet connection."

There are unlimited ways to save, and something for everyone. When browsing with a PC, check out the Firefox or Chrome browser extension; when using a MAC, try out the Safari extension. You can also save from apps like Twitter or Feedly. Pocket is integrated in more than 1,500 apps. The possibilities seem endless, and it's likely that there is a Pocket app or third-party app that will connect. I use Feedly as an RSS feed where I subscribe to my favorite compliance blogs and collect summaries on topics of interest, such as the False Claims Act, compliance program elements, as well as summaries of regulatory information. Feedly is a great way to aggregate information to read on a daily basis, and then save to Pocket to have all the references in one place.

> "...If it's in Pocket, it's on your phone, tablet or computer. You don't even need an Internet connection."

So what's stored in my Pocket? Thank you for asking. My Pocket boasts a number of articles and blogs on Section 1557 of the Affordable Care Act about non-discrimination, information and resources on the CMS Emergency Preparedness Rule, and quick and handy reference articles from HHS on HIPAA (a compliance essential). I use Zapier to connect my Twitter account, but with a twist — I pocket the links on tweets that I "like."

With 30 million users and 2 billion items saved, it may be time for you to demo this popular app. Download it at Apple's App Store, Google Play, or the Amazon Appstore. What's in your Pocket?

HCCA Thanks Our 2018 Compliance Institute

SPONSORS

PLATINUM

ankura
COLLABORATION DRIVES RESULTS

BROAD AND CASSEL

Deloitte.

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Healthicity
Find Simplicity

NAVEX GLOBAL
The Ethics and Compliance Experts

SAI GLOBAL

Wolters Kluwer

GOLD

pwc

KING & SPALDING LLP

Thank you to the 100+ exhibitors
who shared their compliance solutions this year at the Compliance Institute.

COMPLIANCE-INSTITUTE.ORG

HCCA

by Precious M. Gittens and Brett Moodie

A sharpened focus on remediation in federal investigations

» Recent DOJ fraud enforcement trends reveal prosecutors' heightened focus on corporate remediation.

» Remediation is a critical factor in DOJ decision-making in criminal and civil False Claims Act resolutions.

» The DOJ has demonstrated that it will scrutinize an organization's internal reaction to allegations of wrongdoing while it is under investigation.

» Remediation can be of enormous value to organizations seeking "cooperation credit" in both civil and criminal matters.

» Organizations that form a multidisciplinary team to oversee internal investigations and remedial actions may be best-positioned to respond to a government investigation or enforcement action.

Precious M. Gittens *(pmgittens@health-law.com) is Partner and co-chair of the Fraud and Abuse Practice Group in the Washington DC offices of Hooper, Lundy & Bookman, PC.* ***Brett Moodie*** *(bmoodie@health-law.com) is an attorney in the Los Angeles offices of Hooper, Lundy & Bookman, PC.*
bit.ly/in-PreciousGittens *bit.ly/2HfIG61* *bit.ly/in-BrettMoodie*

Today, compliance and ethics programs are an integral part of the operations of many healthcare organizations. These organizations aim to prevent, detect, correct, and in some cases even self-disclose potential fraud and abuse before any misconduct is discovered by government agencies. Sometimes these laudable goals are simply unattainable, and organizations learn about potential misconduct only after the government has detected the wrongdoing and initiated an investigation.

In their investigations of corporate misconduct, federal prosecutors, state and local investigators, and private pay auditors all routinely focus on an organization's preexisting compliance program, along with the organization's remediation and compliance actions *after* it learned of the allegations of misconduct (i.e., after the organization is served with a *qui tam* action, or receives a Civil Investigative Demand, subpoena, or proffer request related to an investigation). Unfortunately, some organizations neglect to do the same, and they tend to look only to the general risks and historical failures, rather than exercising real-time and forward-looking compliance efforts that are focused on remediating the alleged misconduct at hand.

Gittens

Moodie

Failure to engage in remedial actions, including modification of a compliance program that did not detect the allegations that are the subject of a government investigation, can be dangerous. Additionally, an organization that fails to thoroughly, credibly, and promptly investigate and remediate actual misconduct, including misconduct that first comes to the organization's attention as a result of a government investigation, may completely disqualify

itself from later seeking any cooperation credit from prosecutors in federal civil or criminal investigations and enforcement actions.

Historical perspective

The concept of remediation is not new. Indeed, remediation is one of the seven elements of an effective compliance program detailed in the U.S. Sentencing Commission's *Guidelines Manual*.[1] Remediation is also a mitigating factor that impacts the charging decisions, plea offers, and settlements of the U.S. Department of Justice (DOJ). Federal criminal prosecutors are directed to consider ten factors expressly set forth in the *U.S. Attorneys' Manual* (*USAM*).[2] These factors, also considered by federal civil prosecutors, are listed in *USAM* Section 9-28.300, Factors to be Considered, and are commonly referred to among criminal defense lawyers as the "Filip Factors" because they were initially enumerated in a memorandum issued in 2008 by then-Deputy Attorney General Mark Filip.[3]

Filip Factor Number 7 specifically focuses on "the corporation's remedial actions" *after* the potential wrongdoing has been detected. It describes remediation to include "any efforts to implement an effective corporate compliance program or to improve an existing one, to replace responsible management, to discipline or terminate wrongdoers, to pay restitution, and to cooperate with the relevant government agencies." Notwithstanding the well-established concept of remediation, recent DOJ fraud enforcement trends reveal prosecutors' heightened focus on corporate remediation.

Healthcare fraud and abuse enforcement has been heavily influenced in recent years by several interrelated developments in the DOJ. The priorities established by senior leaders in DOJ's Criminal and Civil Divisions have focused on vigorous investigation of individuals, with a parallel emphasis on encouraging organizations to, inter alia (i.e., among other things), operationalize effective compliance programs and take appropriate remedial action.

For more than 15 years, the DOJ has directed prosecutors to pursue cases against criminally culpable individuals responsible for corporate misconduct. In June 1999, former Deputy Attorney General Eric Holder issued a memorandum entitled, "Bringing Criminal Charges Against Corporations" (the Holder Memo), which established the framework that prosecutors use in deciding whether to charge a corporation.[4] The Holder Memo directed prosecutors to "consider the corporation, as well as the responsible individuals, as potential criminal targets" and to consider the corporation's "willingness to cooperate in the investigation." Additionally, the Holder Memo cautioned that "prosecutors generally should not agree to accept a corporate guilty plea in exchange for non-prosecution or dismissal of charges against individual officers and employees."

In September 2015, former Deputy Attorney General Sally Quillian Yates issued guidance to all federal prosecutors regarding an organization's cooperation in the context of corporate investigations (the Yates Memo).[5] The Yates Memo outlines six key steps that prosecutors should take in all investigations of corporate wrongdoing. The Yates Memo directives have been incorporated in the *USAM*, and they are being followed by federal prosecutors in U.S. Attorneys offices nationwide. The Yates Memo reiterated existing DOJ policy and established a new "threshold" for organizations to receive cooperation credit pursuant to the Filip Factors, stating that organizations are required to "identify all individuals involved in the wrongdoing" in order to qualify for *any* cooperation credit in the resolution of a matter. Additionally, the Yates Memo specified that "[t]his condition of cooperation applies equally to corporations

seeking to cooperate in civil matters" such as False Claims Act (FCA) cases.

This "threshold" requirement was a change from the DOJ's prior practice of granting partial cooperation credit to organizations for their significant cooperation, without requiring them to identify the responsible individuals or share all relevant facts implicating those individuals. This new approach to evaluating corporate "cooperation" highlights the DOJ's expectation that organizations will conduct a thorough investigation, disclose evidence of wrongdoing, and take appropriate remedial actions to address the issues identified in the investigation.

This expectation was reinforced further when, at the end of 2015, the DOJ announced the hiring of a full-time consultant, Hui Chen, as the DOJ's first Compliance Counsel Expert.[6] Andrew Weissmann, the former Chief of the Fraud Section of the DOJ's Criminal Division (the Fraud Section) stated that the Compliance Counsel Expert was brought in to ensure that the DOJ was "holding companies to a high but realistic standard," and he emphasized the importance of adding compliance expertise to the DOJ, referring to Ms. Chen as "manna from heaven."[7]

Before her June 2017 departure, Ms. Chen guided, trained, and actively assisted federal prosecutors in making judgements concerning the existence and effectiveness of corporate compliance programs, including whether organizations facing possible criminal prosecution had taken meaningful remediation measures. Additionally, Ms. Chen authored the Fraud Section's "Evaluation of Corporate Compliance Programs" document, which provides sample topics and questions that prosecutors may raise in making individualized assessments of the effectiveness of corporate compliance programs.[8]

Cooperation credit

Building on the DOJ's more discerning review of corporate compliance programs in April 2016, the Fraud Section announced the Foreign Corrupt Practices Act Enforcement Pilot Program (FCPA Pilot Program).[9] The FCPA Pilot Program was designed to incentivize companies to self-disclose potential FCPA-related violations, fully cooperate with the DOJ, remediate flaws in their compliance programs, and disgorge all profits from the improper conduct. In exchange for meeting these requirements, the DOJ offers cooperation credit, a reduction in financial penalties, more lenient charges, and even the possibility of declination of criminal prosecution. In its FCPA Pilot Program guidance, and as adopted into the U.S. Attorneys' Manual in November 2017 as the FCPA Corporate Enforcement Policy, the DOJ defines remediation in the FCPA context as including the:

> [i]mplementation of an effective compliance and ethics program,… [a]ppropriate discipline of employees, and… [a]ny additional steps that demonstrate recognition of the seriousness of the corporation's misconduct, acceptance of responsibility for it, and the implementation of measures to reduce the risk of repetition of such misconduct, including measures to identify future risks.[10]

The FCPA Pilot Program shares the Yates Memo's sharpened focus on meaningful remediation.

Root cause analysis

Most recently, in February 2017, the Fraud Section released its "Evaluation of Corporate Compliance Programs" document. The document contains detailed, sophisticated, and probing questions. For example, the questions related to the first topic set forth in the document, "Analysis and Remediation

of Underlying Misconduct," address the corporation's own root cause analysis of the misconduct, the company's analysis of whether it missed "prior opportunities to detect the misconduct in question," and an assessment of whether the company has engaged in specific remediation to address "the issues identified in the root cause and missed opportunity analysis." The Fraud Section's latest guidance further evidences the DOJ's emphasis on the importance of corporate remediation.

The DOJ has demonstrated that it will scrutinize how an organization is dealing with allegations of wrongdoing while it is under investigation or facing an enforcement action. Organizations that find themselves in that position would then be wise to swiftly and purposefully implement remedial changes. If done well, remediation may enhance the effectiveness of any Filip Factors presentation or separate compliance presentation to the DOJ.

For example, an organization's ability to demonstrate that it has engaged in timely and meaningful remediation in connection with an alleged FCA violation may strengthen its position and arguments in the negotiation of the scope and amount of an FCA settlement. Remediation may also be helpful in responding to audits conducted by governmental or third-party entities, where overpayment settlements often include a component of corrective action. In any case, organizations that are able to demonstrate a clear commitment to their compliance culture, including specific enhancements that have been implemented following an allegation of misconduct, are frequently treated favorably.

Board oversight

Finally, in an increasingly complex regulatory environment and in light of recent DOJ fraud enforcement trends, boards of directors who learn about allegations of misconduct for the first time from any source that is external to the organization would be wise to work with a multidisciplinary team of professionals[11] that can assist the organization in:

- conducting a thorough and credible investigation of alleged misconduct;
- ending any actual misconduct;
- analyzing and addressing how the misconduct occurred in the first place, and why it was not detected by the compliance program; and
- modifying and operationalizing compliance efforts to effectively prevent and detect future similar misconduct.

Conclusion

Remediation lays the groundwork for counsel to initiate substantive discussions with federal prosecutors, and to negotiate and reach a final resolution that may effectively limit the organization's civil liability, reduce its criminal culpability score, or mitigate or altogether eliminate criminal prosecution of the organization and its individual directors and employees.

1. U.S. Sentencing Commission's Guidelines Manual, §8B2.1(b)(7).
2. *United States Attorneys' Manual*, Section 9-28.300, "Principles of Federal Prosecution of Business Organizations" Available at http://bit.ly/2FSjqAb
3. U.S. Department of Justice: Memorandum from Mark Filip, Deputy Attorney General, Principles of Federal Prosecution of Business Organizations. August 28, 2008. Available at http://bit.ly/2nJ5eCU
4. U.S. DOJ: Memorandum from Eric H. Holder, Jr., Deputy Attorney General. June 16, 1999. Available at http://bit.ly/1kyBQWO
5. U.S. Department of Justice: Memorandum from Sally Quillian Yates, Deputy Attorney General, Individual Accountability for Corporate Wrongdoing. September 9, 2015. Available at http://bit.ly/2nLMPa4
6. U.S. DOJ: "New Compliance Counsel Expert Retained By The DOJ Fraud Section" November 3, 2015. Available at http://bit.ly/1Q9sr4I
7. Laura Jacobus: "DOJ's Andrew Weissmann and Hui Chen Talk Corporate Compliance in Exclusive Interview" *ECIconnects* February 2, 2016. Available at http://bit.ly/1P0BpEi
8. U.S. DOJ, Criminal Division, Fraud Section: "Evaluation of Corporate Compliance Programs." Available at http://bit.ly/2lEphmk
9. U.S. DOJ, Criminal Division, Fraud Section: "The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance" April 5, 2016. Available at http://bit.ly/2Dr33KL
10. United States Attorneys' Manual, Section 9-47.120, "FCPA Corporate Enforcement Policy" Available at http://bit.ly/2oSeggM
11. Benson Weintraub: "Integrating White Collar Criminal Defense Lawyers Into Health Care Law Firms to Enhance Corporate Compliance Programs for Optimal Mitigation Under the Federal Corporate Sentencing Guidelines" at 12, Health Care Compliance Association, Compliance Institute, New Orleans, April 2008.

by Sharon Parsley, JD, MBA, CHC, CHRC

Changes to Hospital Inpatient Quality Reporting Program for CY 2018

Sharon Parsley *(sharonparsley@q-a-g.com) is President & Managing Director of Quest Advisory Group, LLC, in Ocala, FL.*

As those of you in the acute care hospital arena may know, CMS continues to refine the measures associated with its Hospital Inpatient Quality Reporting Program. A quick overview of the three areas of most significant change impacting the calendar year 2018 reporting period follows.

Parsley

Hybrid hospital-wide 30-day readmission

For the measurement period January 1, 2018 through June 30, 2018, a voluntary measure of Hybrid Hospital-Wide 30-Day Readmission will be collected during a submission period running from September 1, 2018 through November 30, 2018. Participating hospitals will report on not less than 50% of discharged, age-qualified, Medicare fee-for-service patients. At the current time, the measure will not affect payments, and no public reporting is planned.

Stroke 30-day mortality rate

The Stroke 30-Day Mortality Rate measure has been refined with changes impacting payments made during CY 2023 and beyond. The stroke mortality measure will now incorporate stroke severity codes, which are based on the National Institute of Health Stroke Scale (NIHSS). CMS will also start providing a confidential facility-based feedback report during CY 2021 aggregating claims data from discharges occurring on October 1, 2017 and beyond. It may be worth inquiring about who within your organization is NIHSS certified.

Pain measurement

Last, but certainly not least, the subjective (therefore controversial) pain measurement questions within the Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) survey were further refined. The composite measure itself was renamed to Communication about Pain. More specifically, three of the HCAHPS pain measurement survey questions were modified. Eliminated were questions as to: (1) whether the patient needed medicine for pain; (2) whether pain was well controlled; and (3) how frequently hospital staff did everything they could to help with pain management. The newly added questions ask, during this hospital stay: (1) Did you have any pain?; (2) How often did hospital staff talk with you about how much pain you had?; and (3) How often did hospital staff talk with you about how to treat your pain?

It may be appropriate to evaluate your patient education materials on the subject of pain management and communicating with care providers. Additionally, consider whether your leadership rounding activities should be reassessed so that perceived pain management communication deficits can be addressed on a more real-time basis. If your facility isn't already doing so, drill into performance data in each unit and during each shift. Celebrate successes and perform root cause analyses on low-performing areas.

Lastly, consider whether care team training should be retooled based on these changes to HCAHPS.

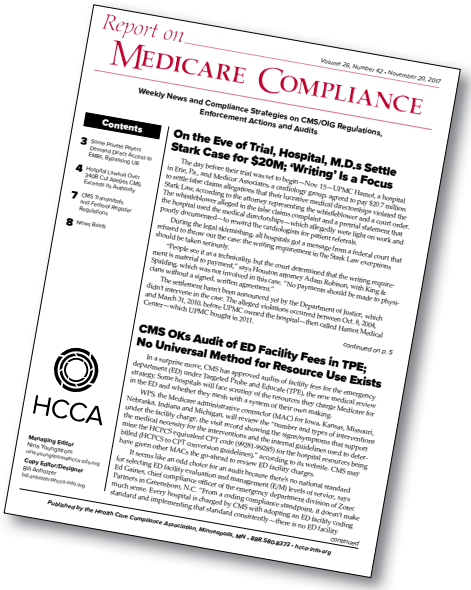
Exclusive Subscriber Content

HCCA PREMIUM NEWSLETTERS

The industry's #1 source of timely news and proven strategies.

Stay current in Medicare, research compliance and patient privacy.

SUBSCRIBE TODAY


Report on MEDICARE COMPLIANCE

Weekly News and Compliance Strategies on CMS/OIG Regulations, Enforcement Actions and Audits

Contents

On the Eve of Trial, Hospital, M.D.s Settle Stark Case for $20M; 'Writing' Is a Focus

CMS OKs Audit of ED Facility Fees in TPE; No Universal Method for Resource Use Exists

HCCA


Report on RESEARCH COMPLIANCE

News and Analysis for Colleges, Universities, AMCs and Other Non-Federal Entities

Contents

NIH: Exceptions to sIRB Policy To Be 'Rare;' 'Compelling Justifications' Still Unknown

Pivotal ORI Misconduct Investigative Chief Resigns; Both Divisions Now Lack Leaders

HCCA


Report on PATIENT PRIVACY

Practical News and Strategies for Complying With HIPAA

Contents

HIPAA Doesn't Mean 'No': McGraw Shares OCR Insights as She Joins Records Start-Up

OCR: After an Opioid Overdose, Sharing Patient Information Can 'Help Save Lives'

HCCA

Award-winning **RMC** provides valuable guidance on where Medicare auditors are going next, how the False Claims Act and Stark Law are being enforced, and what new regulations mean to your organization. Commentary from field experts brings topics to life and gives insight into compliance best practices. Available in print and online.

Member $664
Non-member $763
Weekly—8 pages

SUBSCRIBE
hcca-info.org/RMC
888.580.8373

RRC helps research organizations and investigators understand laws, regulations and funding policies necessary to avoid the negative publicity, financial setbacks and management problems that can result from noncompliance. Available in print and online plus a weekly email with the latest news.

Member $401
Non-member $461
Monthly—12 pages

SUBSCRIBE
hcca-info.org/RRC
888.580.8373

RPP examines the most pressing patient privacy issues. From HIPAA to cyber security to privacy cases moving through courts, **RPP** provides in-depth analysis and practical compliance strategies that will save organizations from costly settlements and damaging patient complaints. Available in print and online.

Member $482
Non-member $554
Monthly—12 pages

SUBSCRIBE
hcca-info.org/RPP
888.580.8373

Published by Health Care Compliance Association

by Gabriel L. Imperato, Esq., CHC and Anne Novick Branan, Esq., CHC

Board responsibility for compliance oversight and program effectiveness

» Board should ensure adequate reporting methods for duty of care, decision-making, and compliance oversight.
» Board must address compliance program resources, structure, and operation.
» Board oversight must focus on compliance program effectiveness.
» Board should have access to healthcare compliance expertise.
» Board should have active and ongoing dialog with compliance professionals and strive to promote an ethical culture in the organization.

Gabriel Imperato *(gimperato@broadandcassel.com) is Managing Partner and* ***Anne Novick Branan*** *(abranan@broadandcassel.com) is Of Counsel in the Fort Lauderdale law offices of Broad and Cassel LLP.*

As the federal government continues to pursue healthcare organizations and dedicate resources to ferret out fraud and abuse, healthcare providers' members of governing bodies must be vigilant in implementing, maintaining, and updating their organization's compliance programs. Fueled by the private whistleblower movement, the potential for government identification of improper practices has resulted in an increased risk of liability for organizations and individuals alike. An expanded duty of care and duty of loyalty underlie what is required from a board of directors (board) to satisfy corporate oversight responsibility standards in a healthcare setting. Both must be satisfied, but the majority of a board's oversight responsibilities fall under the duty of care. Boards must ensure that their organizations have implemented and maintain an "effective" compliance program.

The Federal Sentencing Guidelines for Organizations (FSGO) outline seven elements that are essential to an "effective" compliance program.[1] The second element—Compliance Program Administration—expressly addresses the role of the board and high-level personnel in compliance programs. The board must be "active" and knowledgeable about the organization's compliance program to satisfy the standard. Although the other elements may not expressly implicate the board's responsibilities, it is important to note the "oversight" role extends to other areas. These include the specific provisions surrounding communication, education, and training, as well as monitoring, auditing, and internal reporting systems. As a whole, knowledge regarding content and operations of the compliance program, coupled with oversight of the execution of the program to ensure effectiveness, form the foundation of the duties of the board.


Imperato


Branan

The core of a director's responsibilities in oversight of a compliance program fall under two general prongs: (1) implementation of an effective program; and (2) monitoring of the system in place to ensure timely communication and resolution of potential threats to compliance.[2]

Instituting an effective compliance program

The first step is to institute a compliance program that adequately meets the unique needs of the healthcare organization. There is no one-size-fits-all formula, so a board starting from square one may benefit from professional consultation to navigate the many resources and standards that govern compliance programs.

Prioritizing compliance and communicating a clear message to the employees of the organization from the top down is essential to the success of any program. Creating a culture of ethical conduct and compliance from the beginning not only unifies the diverse membership of an organization in accordance with the compliance goals of the board, but it fosters open communication, which ultimately yields effective risk management. Necessary actions include creating a code of conduct, designating a compliance officer and compliance committee, and conducting a risk assessment to determine and prioritize potential problem areas.[3]

The board may develop a job description for the compliance officer or invite the officer to craft their own description to be submitted for approval.

The Department of Justice (DOJ) has recently published questions for consideration when developing and assessing the effectiveness of a compliance program in its *Evaluation of Corporate Compliance Programs* (DOJ Evaluation).[4] The DOJ suggests first looking at the organization's history, to see how the company has previously designed and implemented new policies and procedures. This includes determining who were the key players involved at the design stage and whether any specific units or divisions were consulted to provide feedback prior to the implementation.

The code of conduct

In its numerous publications, the Office of Inspector General for the Department of Health & Human Services (OIG) has provided general guidance as to what must be included in an organization's code of conduct (code). A code will typically begin with the board resolution that establishes the compliance program. This endorsement from the high-level personnel communicates the organization's clear commitment to the program and shows the active involvement of the board. The code must also clearly outline the standards for expected conduct, as well as the process for handling questions and reporting potential issues, with an emphasis on non-retaliation of those who report concerns. The key in evaluating the process is to look for whether it provides for timely reporting and resolution of compliance concerns. The chain of command for reporting compliance concerns must be described, including the key compliance personnel, not just the organization's compliance officer and compliance committee members. Further, the code should emphasize the organization's zero tolerance policy for fraud and abuse activity, commitment to submitting accurate and timely billing, and compliance with all laws and regulations.

Recently, the OIG (in conjunction with HCCA) published *Measuring Compliance*

Program Effectiveness: A Resource Guide, which provides sample topics and questions for boards to consider in evaluating a compliance program.[5] In the drafting stage, it is suggested that the code of conduct integrate the mission, vision, values, and ethical principles of the organization. Specific elements and statements from the organization's existing documents may be incorporated to increase cohesion and encourage smooth implementation. Once finalized, the OIG encourages a focus on the compliance program's distribution, awareness, and communication. This may be accomplished through a survey of the organization's employees to determine the extent to which they are familiar with the standards contained in the code and how they access it. New employees must be oriented with the policies during the onboarding process.

Assembling a compliance team

The next key role of the board involves the appointment of a compliance officer to oversee the program. The scope of the position will depend on the size and configuration of the organization, although the individual selected should have some background in healthcare, at minimum. The board may develop a job description for the compliance officer or invite the officer to craft their own description to be submitted for approval. Regardless of the drafting method selected, important considerations for the compliance officer's role include ensuring effective prevention and detection of compliance violations, regular review of the program to ensure it is current with government standards, recommending adjustments to the program as needed, reporting to the board, and coordinating resources to ensure the ongoing effectiveness of the program.[6]

A larger organization may require a compliance committee, which would function to assist the compliance officer. Although compliance officers are responsible for the program, they may require additional support in the Compliance department. This support includes education and training, as well as monitoring and auditing personnel. The organization's compliance team works together to ensure that regular risk assessments are conducted, to receive complaints or reports from employees, and to address areas of concern effectively.

As to additional compliance personnel, the board's responsibilities are first implicated at the hiring stage. Independent of subject matter expertise, those selected as compliance personnel must be approachable and have strong interpersonal skills. This encourages open discourse from ground-level employees who will report potential risk areas to the compliance staff. In addition, those who are selected for technical roles, including monitoring and auditing, must have the proper certifications and subject matter expertise (e.g., Certified Professional Coder or Registered Health Information Management Administrator). The OIG encourages that a board prioritize diverse expertise in the members of a compliance committee. Representatives from various departments within the organization, including Operations, Finance, Auditing, Human Resources, Utilization Review, Social Work, Discharge Planning, Medicine, Coding, and Legal, as well as employees and managers of key operating units are needed on the compliance committee.[7] The integration of physicians onto a compliance committee is also an effective way to encourage buy-in from the medical staff. A diverse compliance team yields a strong network to encourage organization-wide accountability and creates a strong culture of compliance from the initiation of the program.

Also critical to assembling an effective compliance team is to maintain the independence of the Compliance department. The

compliance officer may use the resources of the general counsel but should maintain independence in function.

Risk assessment for compliance program design

During the development stage of the compliance program, the board should arrange for a risk assessment to be completed. The target of the assessment is to identify potential problem areas in the current practices and procedures of the organization. This assessment should focus on pinpointing risk factors, identification of potential regulatory and compliance issues, and confirmation of the effectiveness of the compliance controls that are already integrated into the organization's practices.[8] Although there is no single way to complete a risk assessment, the OIG provides various resources that identify potential areas for risk consideration. These include cultural issues; necessity of education and policy revision; billing, documentation, and coding issues; and Stark Law/Anti-Kickback Statute violations, as well as the annual OIG Work Plan and the organization's history of compliance problems.[9,10]

The actual exercise of the risk assessment will likely be delegated by the board to qualified compliance personnel, but the DOJ Evaluation expressly highlights the necessity of participation of business leadership in risk resolution.[11] It is important for directors to receive regular risk reports and for inclusion of risks to be communicated to the compliance committee. Finally, the directors may be responsible for assessment of effective follow-up, if risk resolution falls "off-track."

Funding adequacy

Financial support is crucial to the success of any compliance program. Following the risk assessment, the board is aptly positioned to approve the necessary compliance program budget. The *OIG Resource Guide* provides that a budget must be based on the organization's assessment of risk, with built-in considerations for future program improvement and effectiveness evaluations.[12] The budget must be sufficient to provide the resources for adequate staffing and efficient channels for risk identification and resolution. After the initial budget approval, the OIG suggests that the charter of the board be reviewed with regularity to verify that the approval of the compliance budget is properly documented and accurate.

Determining a budget is not limited to staffing and actual operational costs. The OIG has identified the necessity for boards to establish a plan to keep abreast of the ever-changing regulatory landscape.[13] First, this may be accomplished through education. An investment in the education of the board, key compliance personnel, and all employees and contractors may be a substantial factor in the overall budget calculation. A board may address its subject matter expertise on regulatory compliance by adding to the board or consulting with an experienced legal professional. As a peripheral benefit, the addition of a regulatory, compliance, or legal professional on a board may serve to reinforce the organization's commitment to compliance. The board's ability to properly identify risk factors and ask pertinent questions specific to an organization's industry requires a baseline understanding of the relevant regulatory framework. Thus, an investment by the company in education of the board and key compliance executives is expected.

New considerations may arise post-implementation, when a board evaluates the effectiveness of its compliance program. Assessing the allocation of funding and resources should include how the decisions have been made regarding the allocation of personnel and resources for the compliance and relevant control functions in the past.[14]

The key is to determine whether the allocation comports with the risk profile of the company, as determined through regular audits and compliance reviews. Another suggested area for consideration asks whether there have been times that resources have been denied for the compliance and relevant control functions. If so, boards must consider who was charged with the final decision and what factors were considered in making the determination to withhold resources.

Permissible reliance

Expanding on oversight responsibilities, the OIG has clarified the test as to a board's duty of care. The standard for directors has not been interpreted to require an exercise of "proactive vigilance" or to "ferret out corporate wrongdoing."[15] Rather, the duty of care arises when a red flag is raised or suspicions are, or reasonably should be, aroused. Where the director should have known of the improper activity, failure to act or to become properly informed is what establishes a breach of the duty of care and oversight requirements.

This interpretation paves the way for directors to rely on officers and advisors in conducting their oversight functions. Essentially, where a board is active in reviewing the reports of key compliance personnel, heeding recommendations to maintain and update an effective compliance program, and fostering a culture of compliance within the organization, the oversight role under duty of care will generally be found to be satisfied.

An important caveat to the permissibility of reliance on other personnel is the requirement that directors act in good faith. In the exercise of this duty, the focus must be two-fold: (1) whether there is an improper personal financial benefit that will result from a particular matter or transaction; and (2) whether the director spots any intent to take advantage of the corporation.

If misconduct comes to light, the DOJ Evaluation provides a sampling of questions for directors to consider when analyzing and remediating situation. Directors should analyze the root cause of the misconduct to first identify it, and secondly determine whether it is systemic in nature. The next step may include looking to whether there were any prior indications that would have provided an opportunity to detect the misconduct. Directors should scan audit reports for allegations or identified control failures, complaints, or investigations that involved similar issues. The final stage should address why the organization missed the opportunities to remedy the issue prior to the occurrence of the misconduct.

An important caveat to the permissibility of reliance on other personnel is the requirement that directors act in good faith.

Reporting to the board

The individual assigned the overall responsibility for the compliance and ethics program (i.e., the compliance officer) must periodically report directly to the board on the compliance program activities. The organization's governing authority is required to be knowledgeable about both the content and operation of the compliance and ethics programs in place. With knowledge about the compliance program, the board will be equipped to make inquiries into its structure, operation, and effectiveness. Receiving reports from the compliance officer is essential for the board's exercise of oversight

regarding the implementation and effectiveness of the programs in place. To document the "active" nature of the organization's governing authority, the OIG recommends that the board documents such reports in meeting minutes where the compliance officer reports in-person to the board or to the board's audit and compliance committee on a quarterly basis.[16]

Conclusion

The duty of care compels an organization's board to be active in the process of ensuring compliance. This begins with the institution of a program that effectively addresses the unique concerns of an organization's specialty that is adequately funded and equipped with the necessary resources. The key to satisfaction is to maintain a system that adequately provides the board with information relevant to make decisions. This will not only ensure that the organization meets the federal regulatory compliance standards, but also shields individual directors from personal liability.

The authors would like to acknowledge Bethany Pandher, a law clerk with Broad and Cassel, for her assistance in preparing this article.

1. Federal Sentencing Guidelines for Organizations § 2(a)–(c).
2. U.S. Department of Health & Human Services Office of Inspector General: Practical Guidance for Health Care Governing Boards on Compliance Oversight. 2015. Available at http://bit.ly/2BdHEpw
3. Debbie Troklus and Sheryl Vacca: Compliance 101, 4th edition. pp 50–53.
4. U.S. Department of Justice, Criminal Division, Fraud Section: "Evaluation of Corporate Compliance Programs" February 2017. Available at http://bit.ly/2lEphmk
5. Health Care Compliance Association & Office of Inspector General: *Measuring Compliance Program Effectiveness: A Resource Guide*. March 27, 2017. Available at http://bit.ly/2nFBFCZ
6. Ibid, Ref #3, p 106.
7. Ibid, Ref #3, p 55.
8. Ibid, Ref #2, p 12.
9. Ibid, Ref #3, p 56.
10. OIG website: Compliance Resource Material. Available at http://bit.ly/2E7wOE2
11. Ibid, Ref #5, p 33.
12. Ibid, Ref #5, p 9.
13. Ibid, Ref #2 at 4.
14. Ibid, Ref #2, p 3.
15. OIG & The American Health Lawyers Association: *Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors. 2017.* Available at http://bit.ly/2C0MhzZ
16. Ibid, Ref #5, p 9.

by Jay P. Anstine

Stay current, because the times, they are always a-changin'

Jay P. Anstine *(janstine@bluebirdhealthlaw.com) is the President of Bluebird Healthlaw Partners in Fort Collins, CO.*

April 14, 2003. Hard to believe it's been 15 years since the HIPAA Privacy Rule went into effect. Recently, I had a conversation with a colleague, joking about the days before HIPAA. I recalled a time growing up when the father of a close friend was a physician. I can vividly recall having dinner at their house and seeing stacks of charts sitting on the edge of the table, waiting to be dictated after dinner. A practice now so foreign to us, it'd be appalling by today's standards—completely normal back then.

Anstine

So what's changed? Well, there's the obvious. This was back in the mid-80s, long before HIPAA existed. Another, more subtle change, occurred in society's view of patient information, which unfortunately came at the expense of compromised patient data.

This subtle shift got me to thinking: What other vulnerabilities will come to light that we currently do not know about? That's a scary thought. It is one, though, that I think makes this work exciting, challenging, and ultimately, rewarding. Since we now know the value of health information, it seems the only remaining unknown vulnerabilities are business and technology changes in how healthcare is delivered. While we can't predict the future, part of our work must be devoted to staying current on the development of new business practices and the emerging technologies that facilitate those practices.

So how do we do that? As it relates to new business practices, carve out time within your week to momentarily ignore the regulations and study up on the healthcare marketplace. What new ventures or partnerships are evolving in care delivery? For example, is the recent CVS-Aetna deal the sign of a new trend in cross-sector mergers? If so, how will this impact the safeguarding of patient health information?

If you're not sure which resources to consult for such information, talk with your leaders. Find out where they get their information. As it relates to emerging technologies, a similar approach would be devoting time in your week to studying up on technology-related developments specific to healthcare. If you need assistance in determining where to get such information, talk to your IT and security folks. By staying current in these two areas, it will put you in a better position to anticipate changes within your organization, consult to your leaders who are considering such changes, and mitigate the risks associated with inappropriate safeguards.

by Andrew Amari, JD, CHC and Cornelia M. Dorfschmid, PhD, MSIS, PMP, CHC

Ban the Box: A brief overview of criminal background checks

» Ban-the-Box (BTB) laws exist at the state, city, and county levels with jurisdictional differences.
» Compliance officers need to understand BTB laws' significance for sanction screening.
» Working with HR to assess BTB laws' potential impact is crucial.
» Careful attention to exceptions for healthcare positions is advised.
» Hiring processes must be compliant with BTB.

Andrew Amari *(andrewamari2@gmail.com) is Hospital Policy and Regulatory Specialist at the Association of American Medical Colleges in Washington, DC and* ***Cornelia M. Dorfschmid*** *(cdorfschmid@strategicm.com) is Executive Vice President at Strategic Management Services, LLC in Alexandria, VA.*

Compliance offices do not function alone; they must work closely and frequently with other departments to be effective. Look no further than policies and procedures such as an organization's legal or human resources (HR) working protocol; these common policies are a testament to the amount of interactive work compliance officers encounter. Unsurprisingly, laws, regulations, and rules in non-healthcare areas may demand attention from the Compliance office. Compliance commonly works with HR for issues concerning discipline, hiring, background checks, and sanction screening. For that reason, compliance officers should be aware of a growing type of legislation known as "Ban-the-Box" (BTB) laws.


Amari


Dorfschmid

BTB, a civil rights campaign, has successfully passed its namesake legislation (also known in certain jurisdictions as "Fair Chance" laws) in at least 29 states and 150 cities and counties throughout the United States.[1] California passed a statewide BTB law as recently as October 2017.[2] These BTB laws prohibit employers from running criminal background checks or asking certain questions about criminal convictions during the employment application and hiring process, an area traditionally within HR's purview. However, issues relating to hiring and background checks, which are typically rigorous for those who provide care, require the compliance officer's attention as well. Although BTB laws do not all share the same exact elements, this article details the commonalities among them and the primary varieties within the shared elements.

Jurisdictional BTB distinctions

There are commonalities among most BTB laws. First, each jurisdiction sets a threshold of which organizations the law applies to and which groups of employees are protected by the law. Second, each law prohibits employers from inquiring about criminal history, but at what point the protections kick in during the hiring process depends on the jurisdiction. Finally, each jurisdiction chooses which practices are prohibited and

what information employers are restricted from asking about. Understanding the differences of BTB laws across jurisdictions is crucial to healthcare compliance professionals, especially those who operate in multiple jurisdictions.

Who is subject and who must comply?

BTB prohibitions ordinarily do not apply to an organization unless it employs a number of people specified by the law. Certain jurisdictions require only one employee, whereas others require 25 or more employees before the law's protections begin. Once an organization meets the employee requirement, the BTB's protections apply, and the organization must comply with the BTB law.

The protections also have limitations on who is covered. Although many laws protect applicants to public or private jobs, exemptions are extremely common among BTB laws. Thus, a jurisdiction may define its protected group in several ways. It may provide specific exemptions or enumerate which groups of individuals are covered, therefore implying that unlisted groups are not protected. For instance, certain jurisdictions exempt public employees from the prohibition.[3] Additionally, and most relevant to healthcare organizations, some jurisdictions exempt certain licensed or trade positions or positions that provide care to the young, elderly, or sick.[4,5] Although these exemptions exist, they are uncommon, and healthcare organizations should take care to find out whether the exemption is permitted in their jurisdiction. Other possible exemptions include public contractors, private employers, public safety, fiduciary positions, or when federal or state law says otherwise.

When are practices prohibited?

Timing is one of BTB laws' most distinctive elements across jurisdictions. These requirements dictate when, if at all, an organization is prohibited from making the sorts of inquiries that BTB laws prohibit. This means that certain BTB laws only restrict inquiries about criminal backgrounds until a certain point in the application/hiring process.

The events that trigger protections include, but are not limited to:

- filling out the application (i.e., there cannot be a question regarding criminal activity),
- any time before the interview,
- a criminal background check without an interview (i.e., the interview must occur before the background check is administered),
- any time before offering the applicant a position, and
- before making a decision on whether or not to hire the applicant.[6]

What practices and information are protected?

Each jurisdiction differs in the types of practices that BTB laws prohibit. Generally, BTB laws restrict questions or inquiries regarding an applicant's criminal background. However, each jurisdiction controls exactly which practices it prohibits and to what extent. For instance, BTB laws may prohibit checking for smaller offenses, such as misdemeanors, but not felony convictions.[7] In fact, BTB laws cover a number of different types of criminal history, including convictions, arrests, sealed records, dismissed cases, juvenile records, or diversion programs. Each jurisdiction elects which information its BTB law protects.

The three most common practices that are prohibited under BTB laws are:

- inquiries to an applicant about their criminal background,
- obtaining background checks, and
- using criminal background information in the hiring decision.

All of these items must be considered with the prior information. For instance, although

you cannot run a background check according to some BTB laws, you may be able to do so upon extending a conditional offer of employment to the protected applicant.[8] In that case, the offer may still be revoked after the background check.

Also, where asking about criminal information is prohibited in the hiring process, the practice may not be entirely prohibited. Instead, the law may include exception-based language that allows limited use of the prohibited questioning, such as when "the conviction directly relates to employment." This is true for certain jurisdictions that have addressed their BTB law's relationship to professions with licensure requirements. For instance, New Mexico's BTB law (the Criminal Offender Employment Act) allows any "board or other agency having jurisdiction over employment" to refuse or revoke licensure where the conviction "directly relates" to the particular trade.[9] This means, in certain jurisdictions, the law prevents an organization from disqualifying a candidate from an occupation that requires licensure solely because of a prior conviction, unless the crime bears a specified level (e.g., "direct relationship," "rational relationship," "sufficient nexus") of relation to the job.

Additionally, compliance professionals should familiarize themselves with any laws related to the hiring of caregivers that either create exceptions for the BTB law or lend guidance on how to apply the BTB law to healthcare professionals. New Mexico provides another example with its Caregivers Criminal History Screening Act, which makes clear the limitations of criminal screening for those providing specific types of care. The Act specifies that the criminal history can only be used to see if the applicant has a statutorily defined "disqualifying" conviction.[10]

Exclusion screening

Healthcare providers might also be concerned with exclusion screening as it relates to BTB laws. Exclusion screening through the OIG's List of Excluded Individuals/Entities (LEIE) or state Medicaid Exclusion Lists do not, *per se*, present any issues under the BTB laws. BTB laws are concerned with *criminal* backgrounds, not federal designations. The LEIE serves the purpose of providing a list of individuals who are not allowed to participate in Medicare/Medicaid, and for that reason, it is not necessarily indicative of an individual's criminal history, even if the underlying reason for exclusion is based on criminal action. However, organizations should ensure that their sanction screening question does not implicate criminal history if the state BTB law prohibits it. Instead, organizations should separate questions about exclusions from any language suggesting criminal history will be implicated. Furthermore, certain exceptions discussed above may permit sanction screening in participating jurisdictions. Specifically, exceptions for government licensure bodies, certain healthcare providers, or specific relationships to the job function imply that sanction screening is permitted in these specific instances.

Healthcare providers might also be concerned with exclusion screening as it relates to BTB laws.

Conclusion

BTB prohibitions vary greatly across jurisdictions, whether at the state, city, or county level. Compliance officers should be aware of differences in the scope,

timing, and subject of each law's prohibitive elements. Each organization must ensure that it is familiar with its jurisdictional differences, especially if it operates over many states, cities, and counties. Healthcare organizations must remain cognizant of their obligations under any BTB laws when creating application forms or designing a hiring process, and should coordinate their efforts with HR to comply with applicable BTB laws. Failure to understand when the law applies, at what point in the hiring process it applies, whom it covers, and what information is protected can be detrimental to a healthcare organization's fair hiring process and compliance with the law.

1. National Employment Law Project: "'Ban the Box' is a Fair Chance for Workers with Records" Fact Sheet. August 2017. Available at http://bit.ly/2ErfzKd
2. The National Law Review: "Governor Brown Has Signed 'Ban the Box' Legislation into Law for California" October 17, 2017. Available at http://bit.ly/2EnvfCh
3. National Employment Law Project: "Ban the Box" Guidance. August 2017. Available at http://bit.ly/1T4e72n
4. The City of Lancaster: Employment Application Procedures Memorandum. September 22, 2014. Available at http://bit.ly/2ChZHYG
5. 2017 Minnesota Statutes § 364 (Criminal Offenders; Rehabilitation). Available at http://bit.ly/2Gbias6
6. Ibid, Ref #3
7. California Penal Code §1000.4 (Special Proceedings in Narcotics and Drug Abuse Cases). Available at http://bit.ly/2CiKfLN
8. D C Act 20-422 (Fair Criminal Record Screening Amendment Act of 2014). August 21, 2014. Available at http://bit.ly/2F00Yq8
9. 2006 New Mexico - Statutes § 28-2-4 — Power to refuse, renew, suspend or revoke public employment or license. Available at http://bit.ly/2EDXxYj
10. New Mexico Statute § 29-17-5 (Caregivers Criminal History Screening Act). Available at http://bit.ly/2Hbrj5r

by Frank Ruelas

Downloading software from the Internet

Frank Ruelas *(francisco.ruelas@dignityhealth.org) is a Facility Compliance Professional with Dignity Health in Phoenix.* *bit.ly/in-FrankRuelas* *@Frank__Ruelas*

This month's Security Awareness suggestion deals with raising awareness among computer users on some of the risks associated with downloading software from the Internet. It is not uncommon for downloaded software to create issues that negatively impact a computer's performance. In addition, downloaded software may present a risk to the security of the data on a computer network.

Ruelas

Suggested SAR text

"Please note that software available for download on the Internet may present a risk to the security of the network. Before downloading any software, make sure to contact the Information Technology (IT) department to identify the need for the software, to identify if the software is safe to download, and if its download and use is consistent with IT and company policies."

Why this reminder matters

The Internet has evolved into an important source of information for people. With the continuing development of user-friendly Internet search engines, along with the likelihood that most people have access to the Internet, it is easier for people to find resources that may help them with work-related tasks. One such resource is computer software that may offer the utility to do something that the software currently used does not perform. For example, one popular type of software that people download can create flowcharts, because it is not uncommon for people to need software to draft good quality flowcharts.

> ...downloaded software may present a risk to the security of the data on a computer network.

Where problems occur is when people initiate the download process. Instead of initiating a download, a dialogue box may appear which prompts the computer user to install a download utility program. Sometimes these utility programs do not create any issues, because they simply serve as a router to get the software onto the user's computer. However, this is not always the case. Some of these download utility programs can contain instructions that can track your Internet activity and send it to a third party without your knowledge. They can also record your keystrokes, which can then be used by someone to visit websites and enter your usernames and passwords. These are just a few examples of what can happen when software is downloaded from the Internet. So keep this in mind the next time you are thinking about hitting that "download" button.

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 30,000 emails

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

Visit hcca-info.org/newjobs or call us at 888.580.8373

HCCA™

by R. Stephen Stigall, Esq.

Strengthen compliance to avoid management's liability for opioid diversion

» The government may turn to the Responsible Corporate Officer (RCO) doctrine to prosecute health system executives for failure to detect opioid diversion.

» Under the RCO, management can be held criminally liable for their subordinates' violations of the federal Food, Drug, and Cosmetic Act (FDCA).

» Making disclosures about individuals responsible for diversion as required to earn "cooperation credit" with the DOJ creates a dilemma for management in light of the RCO doctrine.

» In February 2017, the DOJ released compliance program guidance that provides resolution to the dilemma.

» Bolstering compliance to detect and prevent diversion should preclude charges on a RCO prosecution theory.

R. Stephen Stigall *(stigalls@ballardspahr.com) is a Partner with Ballard Spahr LLP in Philadelphia and New Jersey.*

Virtually no one disputes that we are in the middle of an opioid and fentanyl epidemic in the United States. Regardless of where one falls on the political spectrum, there is a recognition that prescription drug abuse is a crisis and is one of the biggest dangers to all of our communities. It leads to addiction, accidental death, and violence in our streets; and the cause of that devastation is in our medicine cabinets—and in controlled substance storage facilities at healthcare institutions.

The United States Department of Justice (DOJ) has recently announced a full-throated response to the crisis, reflecting a clear resolve to use every tool in the government's toolbox to combat prescription drug abuse. Although much of the government's efforts will target the illegal importation of fentanyl compounds manufactured in clandestine laboratories overseas, the government has stated its clear intention to prevent the illegal diversion of highly addictive drugs from healthcare institutions. Diversion is the removal of prescription drugs from intended recipients to others, typically for illicit purposes.[1]

Stigall

There is reason to believe that the government may turn to holding officers, managing employees, and even general counsel of health systems accountable for illegal diversion of opioids under the Responsible Corporate Officer (RCO) doctrine.[2] This may create a dilemma for a healthcare institution's executive staff who, in seeking to avoid prosecution of the business entity through "cooperation credit" by disclosing individual wrongdoing, may simultaneously risk criminal sanction under the RCO, because the conduct occurred under their supervision.[3] *The United States Attorney's Manual* (*USAM*) states, "cooperation is a mitigating factor,

by which a corporation… can gain credit in a case that otherwise is appropriate for… prosecution."[4]

The solution to this dilemma lies in strengthening a healthcare system's compliance program. In February 2017, the DOJ's Fraud Section issued guidance on how it evaluates compliance programs.[5] It would be prudent for healthcare systems to re-evaluate their programs in light of the government's commitment to fighting the opioid crisis with every weapon (and prosecution theory) available.

The government's announced response to the opioid crisis

Since 2016, the government has ramped up its effort to combat the growing opioid epidemic. On September 21, 2016, United States Attorney General Loretta E. Lynch directed all United States Attorneys to draft a district-specific strategy aimed at addressing the opioid crisis.[6] On June 6, 2017, Deputy Attorney General Rod J. Rosenstein addressed law enforcement safety when encountering fentanyl, particularly if it becomes aerosolized and is accidently inhaled.[7] On October 17, 2017, Rosenstein announced enforcement action to interdict deadly fentanyl and other opioids from entering the country;[8] on November 1, 2017, Attorney General Jeff Sessions announced fentanyl safety recommendations for first responders;[9] and on November 9, 2017, the DOJ announced the scheduling of all fentanyl and fentanyl-related analogues as controlled substances.[10] Most recently, on November 29, 2017, Sessions directed each U.S. Attorney to designate an "opioid coordinator" by December 15, 2017 who will: (1) facilitate the intake of opioid and fentanyl cases; (2) convene law enforcement task forces to identify opioid cases for federal prosecution; and (3) provide legal advice and training on opioid prosecutions.[11]

Health systems diversion prosecutions

Historically, the government has prosecuted a number of cases involving diversion of opioids from healthcare systems by a myriad of healthcare professionals. In 2014, Dignity Health agreed to pay $1.55 million to resolve allegations that its compliance procedures and controls failed to prevent diversion of over 20,000 oxycodone tablets.[12] In 2015, Massachusetts General Hospital agreed to pay $2.3 million to resolve allegations that lax controls enabled its employees to divert approximately 16,000 oxycodone pills from automated dispensing machines.[13] In 2016, Appalachian Regional Healthcare, Inc. agreed to resolve allegations that its pharmacy filled improper prescriptions written by an ER physician.[14]

Provider diversions prosecutions

Consistent with the Yates Memo, the DOJ has substantially increased its prosecutions of medical personnel for opioid offenses. On November 8, 2017, the government charged a registered nurse at Abbott Northwestern Hospital, alleging that he accessed secured automated medication dispensing systems, used syringes to remove hydromorphone from vials, and subsequently injected those vials with saline solution to replace the missing hydromorphone.[15] If convicted, he faces four years' imprisonment and a $250,000 fine.[16]

On July 25, 2016, the United States charged a hospice nurse for diverting approximately 42,140 milligrams of oxycodone from Alliance Home Health Care.[17] The hospice nurse pleaded guilty and admitted that her scheme involved: (1) recommending oxycodone for patients who did not need it; (2) arranging for a courier service to hold oxycodone packages so she could pick them up; and (3) recommended hiring another registered nurse who helped the defendant divert and distribute

pills. She faces 24 years' imprisonment and a $1.25 million fine.[18]

Other schemes to divert or steal controlled substances in the hospital setting include: (1) diversion through a "Pyxsis" machine; (2) forging prescriptions; (3) stealing prescription medication from a patient's bedside; and (4) removing medications from the operating room.

The RCO: A potential weapon in the DOJ's arsenal

The RCO is a strict-liability theory of criminal prosecution for violations of the Food, Drug and Cosmetic Act (FDCA) under which the government can prosecute individuals in positions of authority at a company for their subordinates' violations of the FDCA, regardless of their knowledge of or participation in the underlying criminal activity. The seminal cases that established the doctrine are *United States v. Dotterweich*[19] and *United States v. Park*.[20]

In *Dotterweich*, the government charged the Buffalo Pharmacal Company and its president and general manager with introducing misbranded/adulterated drugs into interstate commerce, even though he had no knowledge of the shipments. The jury acquitted the company but found Dotterweich guilty. Upholding Dotterweich's conviction, the United States Supreme Court observed that the FDCA "dispenses with the conventional requirement for criminal conduct—awareness of some wrongdoing. In the interest of the larger good it puts the burden of acting at hazard upon a person otherwise innocent but standing in responsible relation to a public danger."[21]

In *Park*, the government charged Acme Markets, Inc. and its president and CEO with shipping adulterated food in interstate commerce.[22] The company pleaded guilty, and the jury convicted Park at trial. In upholding Park's conviction, the Supreme Court wrote that "the [FDCA] imposes not only a positive duty to seek out and remedy violations when they occur but also, and primarily, a duty to implement measures that will insure that violations will not occur" and that Park had the "responsibility and authority either to prevent in the first instance, or promptly to correct, the violation complained of, and that he failed to do so."[23]

Although the Supreme Court decided *Dotterweich* and *Park* in 1943 and 1975, respectively, the RCO resurfaced within the last 10 years. In 2007, the government charged Purdue Frederick Company, Inc. and its president and CEO, chief legal officer, and former chief medical officer for misbranding OxyContin®, even though the executives were not involved in and had no personal knowledge of the drug misbranding.[24] The executives pleaded guilty and were sentenced to three years' probation, 400 hours of community service, and ordered to disgorge more than $34 million. The executives were also debarred from federal healthcare programs for 12 years.[25]

In 2009, the United States charged Synthes, Inc. and its COO, former president of the Spine Division, former director of Regulatory and Clinical Affairs, and former vice president of operations with shipping adulterated and misbranded bone cement in interstate commerce.[26] The executives pleaded guilty and were sentenced to five to nine months' imprisonment and fined $100,000.

In 2011, the former chairman and CEO of KV Pharmaceutical pleaded guilty to misbranding morphine pills, even though he was unaware of the misconduct and did not intend to violate the FDCA.[27] The judge sentenced him to 30 days' imprisonment and a $1 million fine.

In 2015, the government charged the former CEO and former vice president of sales of Acclarent, Inc., and in July 2016, a jury convicted them of misbranding and

adulteration counts.[28] Sentencing of the defendants is pending.

On May 22, 2017, the Supreme Court denied *certiorari* (i.e., the high court refused to review a decision by a lower court) in *United States v. DeCoster,* which involved the owner and COO of Quality Egg, LLC pleading guilty as "responsible corporate officers" to introducing eggs adulterated with salmonella into interstate commerce.[29] The executives argued at sentencing that imprisonment would be unconstitutional because they had no knowledge of the egg contamination at the time of shipment. They lost. The judge sentenced them to three months' imprisonment and $100,000 fines. On appeal, the executives contended that they were "mere unaware corporate executive[s]." Citing *Park*, the Court of Appeals observed that

> [u]nder the FDCA responsible corporate officer concept, individuals who 'by reason of [their] position in the corporation [have the] responsibility and authority' to take necessary measures to prevent or remedy violations of the FDCA and fail to do so, may be held criminally liable as 'responsible corporate agents,' regardless of whether they were aware of or intended to cause the violation.[30]

The defendants sought review by the Supreme Court. The government successfully opposed the defendants' *certiorari* petition, contending that:

> [1] the duty… on responsible corporate agents is… one that requires the highest standard of foresight and vigilance, [2] the FDCA permits convictions of responsible corporate officials who… have the power to prevent or correct violations of its provisions, and [3] [o]n multiple occasions, Congress has considered whether to amend the FDCA to narrow the scope of liability for responsible corporate agents… but each time opted against any change.[31]

Notably, the government's litigating position regarding the RCO would have been approved at the highest levels in the DOJ.

The government clearly views the RCO as an attractive prosecution theory and could use it to charge health system executives in diversion cases. This may be because the only real defense to the RCO is objective impossibility (e.g., if one was "powerless to prevent or correct the violation"). Indeed, incarcerating management for failing to detect diversion would serve the goal of general deterrence and incentivize health systems to prevent diversion, cutting off at least one source of supply for the illegal drug trade. The FDA's *Regulatory Procedures Manual* states, "prosecutions… against responsible corporate officials, can have a strong deterrent effect on the defendants and other regulated entities."[32]

Prosecutors, however, do not have unfettered discretion to charge individuals under a RCO theory and must first notify and consult with the DOJ's Consumer Protection Branch.[33]

The dilemma for healthcare management

If the government turns to the RCO to fight the opioid crisis, health systems management faces a significant Catch-22. On the one hand, management *must* provide the DOJ all relevant facts relating to the individuals responsible for diversion to qualify for any "cooperation credit" under the Yates Memo, and on the other hand, management could unwittingly point the finger at themselves, given the tenants of the RCO.

Topics prosecutors consider

How, then, can health systems managers resolve this tension? The government has suggested the answer in the DOJ Fraud Section's

February 2017 guidance. That document explains how the DOJ evaluates the effectiveness of compliance programs and remedial efforts to implement or improve one. Although it is not a rigid checklist or formula, it summarizes the topics prosecutors typically consider when evaluating such programs and identifies the questions prosecutors ask for those evaluations. A health system would be wise to evaluate its compliance program against the topics and questions in the guidance.

Analysis and remediation of underlying misconduct
Has the company undertaken a root-cause analysis of the underlying misconduct? What has that analysis shown? If there were prior opportunities to ferret out the misconduct, why were those opportunities missed? Have changes been implemented to reduce risk of reoccurrence?

Senior and middle management
Is there truly a culture of compliance throughout the organization? Do senior leaders and management model proper behavior?

Autonomy and resources
Does the compliance function act independently within the organization? Does it receive adequate resources in funding and personnel?

Policies and procedures
Who designed and implemented the policies and procedures? How does the company communicate them? How accessible are they? Have they been operationally integrated?

Risk assessment
What methodology has the company used to identify and analyze risk? Did the information and metrics detect or miss the underlying wrongful conduct? If the latter, what steps has the company taken to mitigate risk?

Training and communications
Have high-risk and control employees received training that addresses the risk where the misconduct occurred? Have senior management made the company's position clear on misconduct and made resources available for employees to consult on compliance policies?

Confidential reporting and investigation
Has the company collected, analyzed, and used information from its reporting mechanisms and assessed the seriousness of the allegations received? Was the ensuing investigation conducted independently and objectively by qualified personnel with full access to the reporting function? How high within the company is reporting and investigation escalated?

Incentives and disciplinary measures
What discipline did the company impose in response to the misconduct and when did it do so? Are managers held accountable for misconduct that occurred under their supervision? Who participates in the disciplinary decisions? Is discipline imposed fairly and consistently across the organization?

Continuous improvement, periodic testing and review
Has the company learned from its mistakes? Has it periodically tested its vulnerabilities, reviewed the results, and made systemic improvements in its controls?

Third party management
Has the company appropriately managed its third parties to mitigate risk as part of its compliance program?

Mergers and acquisitions
Was the misconduct or risk of misconduct identified during the due diligence process? Has the compliance function been

consolidated into the merger, acquisition, and integration process?

Resolution: Evaluation/strengthening of compliance program

With the foregoing topics as a backdrop, a health system can take several steps to establish or enhance its compliance program to mitigate opioid diversion, such as conducting comprehensive background checks and investigations of its employee candidates. Concomitantly, health systems should report individual employee's obvious wrongful conduct to state and local law enforcement and to an employee's future employer. Doing so will prevent diverters from taking advantage of an industry that naturally resists disclosure, given HIPAA and privacy concerns, which otherwise results in diverters freely moving from employer to employer, undetected, and simultaneously putting the institution and community at risk. Moreover, concealing diversion from the authorities invariably will result in far-worse consequences.

A health system should impose pre-employment drug testing for candidates and random, periodic drug testing for all employees. The company should also order testing for specific opioids in addition to common street drugs. Although specific tests cost more, a prosecutor will distinguish between the company that tests to mitigate specific risks and the company that skimps in an effort to save a few extra dollars.

Health systems must regularly audit opioid dispensing mechanisms and storage facilities and address head-on the audit's findings. The company should determine why dosage/unit counts are off and how the controlled substances went missing. The company should also test vials/ampules of liquid opioids to see whether they have been surreptitiously replaced with saline or water.

A health system should also carefully consider the placement of its opioid dispensers/machines. Diverters easily take advantage of machines placed in isolated rooms, out of public view, or near bathrooms where the diverter can quickly hide after stealing the medication. Placement that increases the risk of detection is best. Security cameras installed near the dispensers will also have a strong deterrent effect.

Finally, management should train all employees and third parties about diversion and prevention. Senior leaders likewise should instill a zero-tolerance culture against diversion, and, if misconduct is uncovered, permit an independent and objective investigation by qualified personnel.

1. *United States v. Moore*, 423 U.S. 122, 135 (1975).
2. *United States v. Park*, 421 U.S. 658 (1975).
3. Memorandum from Sally Quillian Yates, Deputy Attorney General: "Individual Accountability for Corporate Wrongdoing" September 9, 2015. Available at http://bit.ly/2tSoJh8
4. *United States Attorneys Manual*, §§ 9-28.210; 9-28-300; 9-28-700
5. U.S. Department of Justice Criminal Division, Fraud Section: Evaluation of Corporate Compliance Programs. 2017. Available at http://bit.ly/2o03nZ5
6. Memorandum from Loretta E. Lynch, Attorney General: "Department of Justice Strategy to Combat Opioid Epidemic" September 21, 2016. Available at http://bit.ly/2EChSKr
7. DOJ: Justice News press release: "Deputy Attorney General Rod J. Rosenstein Delivers Remarks on DEA Fentanyl Guidance" June 6, 2017. Available at http://bit.ly/2EHlpLG
8. DOJ: Justice News press release: "Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Enforcement Actions to Stop Deadly Fentanyl and Other Opiate Substances from Entering the United States" October 17, 2017. Available at http://bit.ly/2oib6Tb
9. DOJ: Justice News press release: "Statement by Attorney General Sessions on Fentanyl Safety Recommendations for First Responders" November 1, 2017. Available at http://bit.ly/2GsEnC0
10. Drug Enforcement Administration, press release: "Department of Justice Announces Significant Tool in Prosecuting Opioid Traffickers in Emergency Scheduling of All Fentanyls" November 9, 2017. Available at http://bit.ly/2FhgBcI
11. Memorandum from Attorney General Jeff Sessions: Designation of Opioid Coordinators. November 29, 2017. Available at http://bit.ly/2EPrZij
12. United States Attorney's Office, Eastern District of California, press release: "Dignity Health Agrees to Pay $1.55 Million in Civil Penalties to Resolve Controlled Substances Act Claims" July 16, 2014. Available at http://bit.ly/2oj1Myt
13. Settlement Agreement between United States and Massachusetts General Hospital. Sept. 28, 2015 at 8, Attachment 2, Statement of Relevant Conduct. Available at http://bit.ly/2EDvSHN
14. *United States v. Appalachian Regional Healthcare*, Inc., Civ. No. 5:16-cv-00132-JMH, (E.D. Ky. May 2, 2016), Complaint, at Docket Entry No. 1.
15. See *United States v. Amundson*, Crim. No. 17-283-SRN-DTS, (D. Minn. Nov. 8, 2017), Indictment, Docket Entry 1.
16. See 21 U.S.C. §§ 843(a)(3) and (d)(1).
17. *United States v. Ulibarri*, Crim. No. 16-cr-03486-JB, (D.N.M. Jul. 25, 2016), Criminal Compl., Docket Entry 1.
18. See 21 U.S.C. §§ 846, 841(a)(1) and (b)(1)(C), 843(a)(3) and (d)(1).
19. *United States v. Dotterweich*, 320 U.S. 277 (1943).
20. *United States v. Park*, 421 U.S. 658 (1975).
21. Dotterweich, 320 U.S. at 278, 286.
22. Park, 421 U.S. at 658.
23. Id. at 658, 674.
24. *United States v. Purdue Frederick Co., Inc.*, 495 F. Supp.2d 569 (W.D. Va. 2007).
25. *Friedman v. Sebelius*, 686 F.3d 813, 828 (D.C. Cir. 2012).
26. *United States v. Norian Corp., et al.*, Crim. No. 09-cr-403-LDD, (E.D. Pa. Jun. 16, 2009), Indictment, at 54, Docket Entry 1.
27. *United States v. Hermelin*, Crim. No. 4:11-CR-85-ERW, (E.D. Mo. Mar. 10, 2011), Information, at 7,8, Docket Entry 1..
28. *United States v. Facteau*, et al., Crim. No. 15-cr-10076-ADB, (D. Mass. Apr. 8, 2015), Indictment, Docket Entries 1, 432.
29. *United States v. DeCoster*, 828 F.3d 626 (8th Cir. 2016, cert. denied, ___ U.S. ___, 137 S. Ct. 2160 (2017).
30. Id. at 632 (citing Park, 421 U.S. at 673-74).
31. Brief for the United States in Opposition, *DeCoster v. United States*, at 10 (filed Apr. 12, 2017) at 10-11, 23, 24 (citing S. Rep. No. 684, 94th Cong., 2d Sess. 30 (1976).
32. FDA's *Regulatory Procedures Manual* at §6-5-3. Available at http://bit.ly/2C98AYU.
33. See *USAM* §4-8.200.

by Bethany A. Corbin, JD

Data breach compliance after Uber: Avoiding scandal

» Data breaches are inevitable, but compliance responses can mitigate damage.
» Breach notification alone should not drive the investigation process.
» Inventory your sensitive data to identify system vulnerabilities.
» Incident response plans can lead to effective breach response strategies.
» Breach validation and containment are crucial to mitigation.

Bethany A. Corbin *(bcorbin@wileyrein.com) is an attorney at Wiley Rein, LLP in Washington, DC and focuses her practice on healthcare, privacy, and cybersecurity.*

Like the latest installment of the *Star Wars* saga, data breaches are highly anticipated, command strong media attention, and can impact the lives of millions of consumers. From Anthem Blue Cross to Banner Health to Equifax, security-related incidents have dominated headlines and remain a top concern for businesses in 2018. In a survey of more than 15,000 chief information security officers (CISOs), the Ponemon Institute found that 67% of CISOs believed their companies would likely experience a cyberattack or data breach this year, with 60% noting that their concern has increased since 2017.[1,2]

Healthcare entities in particular are prime targets for data breaches, given the sensitive information contained in medical records. From January to June 2017, hackers accessed almost 1.6 million patient records, and insider wrongdoing further exposed another 1.17 million patient records.[3] Failure to appropriately secure data and implement timely responses and notification measures for breaches can expose healthcare organizations to reputational damage, investigative inquiries, and civil liability. Given the organizational risks associated with data breaches, it is unsurprising that the term conjures images of fear for both companies and consumers, much like the *Star Wars* Death Star inspired dread throughout space civilizations.


Corbin

The inevitability of data breaches has forced companies to question their prevention and response strategies—particularly in light of Uber's recent data breach scandal. Although the popular press has taken issue with Uber's failure to follow data breach notification laws, adherence to such laws alone will not ensure a culture of compliance—especially in the healthcare industry. Rather, an effective compliance response to healthcare data breaches must begin before a breach occurs and continue after the breach is contained. Breach notification is an important aspect of compliance, but contrary to widely held belief, it should not dominate the compliance and investigative process. Instead, organizations

must focus on identifying, containing, and remedying the breach as top priorities. This article proposes three compliance strategies for healthcare entities to employ before, during, and after a data breach to help avoid becoming the next Uber.

Before a data breach

Knowing what kinds of protected information your organization handles, where it is stored, and who handles it and why (both in-house and with vendors) is key to keeping that data safe. An incident response plan will help you respond effectively to a possible threat.

Inventory and monitor protected health information

If your organization collects, maintains, or uses protected health information (PHI) (as that term is defined by the Health Insurance Portability and Accountability Act [HIPAA] and relevant state law), you should review and analyze your information systems to identify where your company stores PHI and other sensitive data.[4] An inventory of protected information can help confirm your compliance with state and federal laws. This inventory should provide a complete summary of every element of PHI that your organization possesses—in both paper or electronic format. An easy way to begin the inventory is to follow the path of PHI through your organization from the time a patient contacts your organization until the final claim is paid, accounting for each person and system that handles PHI. Consider documenting the types of PHI and sensitive information that your organization maintains and how this data is kept secure. By understanding the flow of sensitive data, your organization can respond faster to a breach and will have an immediate sense of whether the system hack involved sensitive information. Following this inventory, you should continue to review and update your information systems, and monitor for PHI and data leakage or loss.

Develop an incident response plan and risk mitigation strategy

An incident response plan (IRP) is a key organizational document that converts knowledge into a step-by-step actionable framework for use during a data breach. In essence, the IRP should be a written data breach response policy that identifies the appropriate individuals to contact during a breach, sets forth required documentation efforts, and highlights response strategies. Legal standards, including breach notification requirements, should also be incorporated into this document.

Consider identifying the appropriate incident response team in the IRP, which may include the chief privacy officer, general counsel, administrators, IT professionals, and risk management representatives. The individuals on the team should be empowered to react to a data breach, and should receive applicable training on data breach response and mitigation. Further, your IRP should specify incident handling procedures and should ensure that all employees know how to timely report data breaches. Ensuring effective internal communication is key during a data breach, and each employee should be reminded of the time sensitivities associated with compromised PHI. When they occur, data breaches are stressful events, and the creation of a well-executed IRP can minimize the impact and uncertainty associated with a breach.

Assess and understand vendor vulnerabilities

In the age of outsourcing, most healthcare organizations rely heavily on approved vendors to conduct certain business operations. As the Health Information Technology for Economic and Clinical Health (HITECH) Act

made clear, business associates that work for covered entities and have access to PHI must comply with HIPAA. The HITECH Act expanded liability for both business associates and covered entities in the event of a breach, and covered entities may be liable for breaches that occur within the vendor organization.

Accordingly, it is crucial that covered entities understand their legal and compliance obligations with respect to vendors. Indeed, the Equifax hack recently exposed theoretical healthcare vendor vulnerabilities.[5] Equifax operates as a financial verification vendor to the Department of Health and Human Services for enrollees under the Affordable Care Act. Equifax's marketplace exchange data was not implicated in the breach, but it serves as a cautionary tale of how vendors can leave covered entities vulnerable to attack. Healthcare data breaches premised on vendor vulnerabilities are increasingly common, and data sharing with third parties is perceived as one of the biggest vulnerabilities for healthcare providers. Thus, covered entities should attempt (to the best of their ability) to actively monitor their vendor's privacy and security compliance, and ensure that effective and clear lines of communication exist for vendors to report data breaches to the covered entity.

If it's too late to prevent a breach, you should focus on taking steps to minimize the impact and limit further damage.

During a data breach

If it's too late to prevent a breach, you should focus on taking steps to minimize the impact and limit further damage.

Validate and contain the breach

When faced with a data breach, your organization should respond immediately to verify and contain the breach.[6] The goal here is to stop the bleeding as swiftly as practical. Identify the affected systems and work to segregate affected servers or endpoints. Determine the type of information disclosed and its sensitivity level, which will help guide your mitigation plan and subsequent notification requirements, if any. Not every breach will involve PHI, and it's important to recognize the level of confidentiality associated with the breached data. Further, you should evaluate whether the breach is ongoing (e.g., system hack) or sufficiently limited in scope (e.g., lost flash drive or laptop). If the breach is continuing, take immediate action to prevent further data loss.

Consider isolating and containing any infected system to prevent additional damage until a long-term solution can be devised. If the breach involved a loss of property, such as a laptop containing PHI, investigate whether the device can be recovered. If recovery is successful and it is evident that the sensitive data had not been accessed, breach notification may be unnecessary.

Implement your incident response plan

After taking steps to contain the immediate breach threat, your organization should implement its IRP. The IRP will specify notification procedures for the incident response team, and these individuals must be apprised of the status of the breach and any efforts taken to contain or stop the breach. Effective internal communication during and after a breach is essential to mitigate damage, and the incident response team will likely need to coordinate communication among multiple organizational units. Additionally, be sure to

document all mitigation efforts and response measures, as this will be crucial for evaluating the effectiveness of your IRP and can serve as favorable evidence in a subsequent investigation.[7]

Notify legal counsel and insurers

With the breach contained and your IRP implemented, you should determine if notifying legal counsel and relevant insurance companies is warranted.[8] Involving an attorney at an early stage in the breach investigation will permit maximum use of the attorney-client privilege. This doctrine limits access to certain privileged communications between attorneys and their clients, and it can prevent those communications from being disclosed during subsequent investigations or lawsuits.

The lawyer you contact should be familiar with your company's business structure, operations, policies, and risk management plan, and should also possess substantive knowledge of data breach laws. In addition to notifying your attorney, you should also alert any relevant insurance companies that a breach occurred. Insurers have extensive experience dealing with data breach mitigation and may offer helpful strategies and suggestions. Data breaches often grow in scope and size from what is originally anticipated, so involve your insurer early—even if you don't think the damage from the breach will exceed your policy's limits.

After a data breach

After the fire is out, you may need to notify the appropriate federal, state, and local authorities, as well as the consumers affected by the breach. A post-mortem of your response plan will also help you make improvements and demonstrate that your organization is serious about handling breaches.

Investigate and fix vulnerable systems

Following the immediate aftermath of a data breach, it is necessary to investigate the cause of the breach and mitigate harm. Learn as much as possible about the root cause of the breach. For example, if a laptop containing PHI was stolen, determine how an unauthorized individual obtained access to the laptop. Were there insufficient physical controls, such as locks, that enabled access? This investigation may require the involvement of technical specialists and professionals, including forensic investigators.

Even if a data breach is limited in scope and contained, it is essential to determine why the breach occurred and remedy the underlying vulnerability. Liability for data breaches is often more severe if an organization had knowledge of a vulnerability but failed to fix it, and insurance companies may refuse to cover breach incidents where the company purposefully failed to act in light of this information. Data breaches should thus be viewed as an opportunity to remedy vulnerabilities and enhance organizational security.

Comply with breach notification laws

Once your organization has investigated the cause of the breach and determined whether PHI was exposed, it's time to address compliance with breach notification laws. The HIPAA Breach Notification Rule is a comprehensive regulation that outlines organizational procedures for the unauthorized use or disclosure of PHI, and the majority of states have enacted their own breach notification statutes. Accordingly, healthcare entities may be subject to two or more breach notification standards, depending on the relevant jurisdiction(s). HIPAA does not preempt more stringent state laws, and numerous state statutory frameworks specify the required contents of a breach notification. Notification under HIPAA may take a slightly different form

than notification under state law. The legal counsel you consulted during the breach can assist with navigating the technicalities of these laws.

Although healthcare organizations must comply with both federal and state laws, not all breaches require notification. For instance, although PHI may have been contained on a stolen laptop, HIPAA and most state statutes do not require notification if the PHI was encrypted and the encryption key was not similarly accessed.[9] Additionally, some breach notification statutes incorporate a risk of harm analysis, and if the risk of harm to consumers is sufficiently low, notification is not required. Be sure to check local regulations for documenting this risk of harm analysis, and ensure that consultation with a relevant state agency is not required. It's important to review the federal and state laws directly applicable to your organization to determine if breach notification is even a relevant concern. If notification is required, consider involving your Marketing or Public Relations department to help craft notification statements and press releases.

Review and revise the incident response plan

Finally, it's important to analyze the effectiveness of your IRP after it has had a chance to work in action. Did your IRP work smoothly? Were there glitches in communication that need to be resolved? What improvements can be made? Every data breach incident is a learning experience, and you should take time to consider the strengths and weaknesses of your IRP. The early documentation that you kept in implementing the IRP can be particularly helpful in determining where improvements can be made. Understanding and fixing weaknesses is essential to enhancing organizational security and goes a long way towards demonstrating a strong commitment to compliance.

Conclusion

The threats associated with data breaches are daunting. As the healthcare industry becomes increasingly connected, these threats will multiply in number and magnitude over the coming years. We can't use the "force" to stop data breaches and hackers, but organizations can strengthen their internal security controls, response plans, and compliance frameworks to handle breaches in a comprehensive and effective manner. By implementing effective compliance controls, organizations can guard against scandal and improve the security of patient data.

1. Opus: "What CISOs Worry About in 2018: A Ponemon Institute Survey, January 9, 2018." Available at http://src.bna.com/vAu
2. Jimmy H. Koo: "Data Breaches Remain Top Concern for Chief Information Security Officers in 2018" *BNA Privacy & Data Security Blog*; January 11, 2018. Available at http://bit.ly/2Dync1N
3. Protenus, Inc.: "2017 Breach Barometer Report: Mid-Year Review" Available at http://bit.ly/2nEbP1y
4. See Privacy Technical Assistance Center: Data Breach Response Checklist. Available at http://bit.ly/1hon1tn
5. Dave Barkholz: "Equifax Breach Exposes Healthcare Vendor Vulnerabilities" *Modern Healthcare*; September 12, 2017. Available at http://bit.ly/2r6Ghpf.
6. Kirk Nahra and Edward Brown: "Responding to Security Breaches" *The Practical Lawyer*; October 2016. Available at http://bit.ly/2DhTq3r.
7. Robert Lord: "You've Had a Health Data Breach – Now What?" *Compliance & Ethics Blog*; February 14, 2017. Available at http://bit.ly/2EJQNVs.
8. Ibid, Ref #6, at 41.
9. 45 C.F.R. § 164.402 (Modified definition of a breach, effective March 26, 2013)

by Marti Arvin

Business associates: Have you really integrated them into your risk profile?

» When applicable, business associate agreements (BAA) that meet all of the regulatory requirements must be in place.

» Having an appropriate BAA does not necessarily mitigate the risk for the covered entity.

» The BAA should require the associate to notify the covered entity of incidents that involve a violation of the HIPAA Privacy or Security Rules.

» Covered entities should determine if a business associate's data compromise is a breach.

» Covered entities must exercise ongoing due diligence for business associate compliance.

Marti Arvin *(marti.arvin@cynergistek.com) is Vice President of Audit Strategy at CynergisTek in Austin, TX.*

When the HIPAA Privacy Rule became enforceable in April of 2003, many organizations made efforts to assure a business associate agreement (BAA) was in place when a vendor was clearly going to handle protected health information (PHI). However, the level of effort was quite varied. Since that time, organizations have increased and improved on these efforts. With the changes under the HITECH Act[1] and the corresponding implementing regulations, organizations updated their agreements and made efforts to get newly signed BAAs with current vendors by the September 23, 2014 deadline.

Arvin

In April of 2012, the Office for Civil Rights (OCR) entered the first Resolution Agreement and Corrective Action Plan (RA/CAP) that involved a finding regarding the lack of a BAA.[2] Still, many organizations did not give this significant attention until OCR began its Phase II audit process in the beginning of 2016. One of the initial steps of that process asked covered entities to provide a list of their business associates. This request had some covered entities scrambling to produce the list and questioning the completeness of their list. Later in 2016, OCR had its first RA/CAP that involved the failure to update a BAA in a timely manner.[3] The resolution amount was $400,000. Almost exactly six months later, another agreement was entered with OCR over the failure to obtain a BAA.[4] This time the amount was only $31,000.

All of this demonstrates the regulatory obligation to assure that when a covered entity engages a vendor to perform a service for or on its behalf and the vendor will create, receive, maintain, or transmit PHI in the performance of said activities, the covered entity will obtain satisfactory assurance that the business associate will appropriately safeguard the information.[5] These assurances are obtained through a BAA. However, obtaining a BAA that meets the regulatory provisions may not be sufficient to appropriately address risks.

Implications to the covered entity's risk profile

Although an organization might be doing a good job of getting a BAA in place, that is not enough to fully address the risk a business associate relationship may pose to the covered entity. This is not a one-and-done undertaking. The assessment of how the business associate fits in to the covered entity's risk profile is an ongoing process throughout the life cycle of the relationship. It starts with the due diligence necessary prior to beginning the relationship and goes through the processes needed to end the relationship. Questioning the business associate's compliance during this entire process is necessary to accomplish this.

The regulations require the covered entity to obtain satisfactory assurances through the BAA, but there is no guarantee the business associate will appropriately safeguard the information. Further, other than the mandated provisions of a BAA, there is no definition in the regulations that clarifies what the "satisfactory assurances" must be. OCR has clarified through its FAQ process that a covered entity is not obligated to monitor how a business associate specifically is safeguarding the covered entity's data. However, failure to perform any due diligence can create risks for the covered entity. Let's look at one example to demonstrate this—a data compromise at the business associate.

Under the HIPAA Security Rule, a BAA must include a provision requiring the business associate to notify the covered entity of any security incidents.[6] The rule defines a security incident as "the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with systems operations in an information system."[7]

Most organizations have dozens if not hundreds of business associates. Although all of the vendors who fit the definition of a business associate might not have large volumes of an organization's PHI, a significant percentage will. Most organizations I speak with have had very few notifications from their business associates of a security incident. In that same vein, I have encountered very few organizations that believe their business associates are not being impacted by the same cybersecurity issues as others in the healthcare space.

Why are there so few reports of security incidents by vendors?

The answer to the question could be quite simple. Either the vendors don't know about the attempted or actual cyberattacks on their systems, or they know but are not reporting them. Whichever it is has implications to the risk profile for the covered entity.

Another consideration is whether, as a covered entity or a business associate with a downstream subcontractor, the only interest is in security incidents. By definition, a security incident only involves electronic PHI (ePHI). If the BAA only discusses the need to notify the covered entity of "security incidents," the vendor has no explicit obligation to notify the covered entity of other types of data incidents, such as those involving improper access to paper or verbal information and/or use, disclosure, and modification or destruction of PHI.

Many might think this issue of reporting only security incidents is resolved by the requirement of the HIPAA Breach Notification Rule that states a business associate must notify a covered entity of a breach without undue delay but no more than 60 days after discovery. However, this provision may still not lead to the covered entity being notified by the business associate of non-security incident data compromises.

This is because the rule only requires the business associate to notify the covered entity of a "breach." A breach, as defined by the regulations, means an assessment has already occurred to determine whether notification is

required.[8] This means if the BAA requires the business associate to notify the covered entity of a breach, the business associate is determining whether notification is required. If the business associate makes a determination that a notice is not required, the obligation to notify the covered entity is not triggered. This could be a problem for the covered entity.

If the business associate assesses an incident and determines no breach occurred, the covered entity has the liability for failure to timely notify the affected individuals and the OCR if the business associate is wrong. The regulatory provisions in the HIPAA Breach Notification Rule make it the obligation of the covered entity to notify individuals and the OCR when a breach occurs.[9] This is not the obligation of the business associate. The business associate's obligation is to notify the covered entity.[10] This is why it is important to assure the language of the BAA protects the covered entity and that covered entities are proactive in assuring business associates are meeting their obligations.

Covered entities should also be monitoring any reported incidents of data compromises at their business associates.

Covered entities should be proactive

The BAA language should require that the business associate notify the covered entity of all possible or actual data compromises, not just security incidents. The language should further clarify that, while the business associate is obligated under the HIPAA Breach Notification Rule to notify the covered entity of a breach, the covered entity should also be notified of any instance where the business associate assessed a situation and determined it was not a breach. Some organizations include language that requires the business associate to notify them of any HIPAA Privacy or Security Rule violation as a way of handling this issue. Once a covered entity is notified of an incident, it should be initiating interactions with the business associate to learn as much as possible about the nature of the incident, what data might have been compromised, and what the business associate is doing to handle the incident. Covered entities should also consider language that clarifies their right to make a final determination whether the incident is a breach and thus requires notification to the affected individuals and OCR.

Covered entities should also be monitoring any reported incidents of data compromises at their business associates. Once a data compromise has been publically reported, such as through the media, the incident is likely deemed discovered by the covered entity. For example, if the media reports that a business associate was the victim of a ransomware attack, covered entities should be reaching out to the business associate to determine what happened. Ransomware attacks are particularly significant. Whether a ransomware attack is a breach was debated by the industry until the OCR issued guidance on the topic.

The OCR guidance is that a ransomware attack is very likely a compromise of any PHI on the systems impacted by the attack.[11] The guidance tells us that if ePHI was encrypted by the attacker, it means the attacker has acquired the data, because they have taken possession or control of the ePHI. This acquisition by the attacker is a disclosure that would not otherwise be permitted by the Privacy Rule. There is some room in the guidance for a determination that the attack was not a breach if the covered entity or business associate

can demonstrate the data was not "accessed" or "exfiltrated" by the attacker. However, the guidance seems to imply the evidence of this must be very strong before an organization can say there is a low probability of compromise.

Because the regulations place the duty to notify on the covered entity, it is critical the covered entity be aware of what the business associate is doing and carefully review the determinations made by the business associate. A covered entity should carefully consider whether it will allow the business associate to be the final decision-maker regarding whether a breach has occurred. If the business associate's position is that no breach has occurred, the covered entity should ensure they are very confident in the evidence the business associate has used to demonstrate the low probability of compromise.

Although the covered entity, through the BAA, might transfer the activities and/or cost associated with breach notification to the business associate when the incident is the result of the business associate's acts or omissions, the legal responsibility to notify remains with the covered entity. This is why it cannot be emphasized enough that once the covered entity discovers that its business associate has had a data compromise, the communication channels are opened, and the discussions begin to ensure breach notification, if required, is done within the regulatory timeframe. The covered entity needs to assure the business associate is taking prompt action. The covered entity should question whether appropriate system analysis and forensics have been done. They should also know what steps have been taken to identify the data impacted. Failure of the business associate to act promptly can quickly absorb the limited time period for notification.

Conclusion

Covered entities may wish to reassess and/or update the language of their BAAs regarding what types of incidents the business associate must notify the covered entity about and the timing of such notification. They should also consider the language regarding who is responsible for what, if a data compromise like a ransomware attack occurs. Covered entities should not just rely on a statement from the business associate that notification is unnecessary. This is definitely a "trust, but verify" situation. Getting a valid BAA with a vendor may satisfy the regulatory obligations for the covered entity, but it does not necessarily eliminate the risk to the covered entity. Ongoing diligence through the entire relationship is a must.

1. Health Information Technology for Economic and Clinical Health (HITECH) Act Interim Final Rule. February 17, 2009. Available at http://bit.ly/2gu0mNS
2. U.S. Department of Health and Human Services, Office for Civil Rights: Resolution Agreement - Phoenix Cardiac Surgery. Available at http://bit.ly/2FEwF7q
3. DHHS, Office for Civil Rights: Resolution Agreement and CAP - Women and Infants Hospital. 2016. Available at http://bit.ly/2nD7JWz
4. DHHS, Office for Civil Rights: Resolution Agreement and CAP – Center for Children's Digestive Health. 2017. Available at http://bit.ly/2pA8Cm3
5. 45 C.F.R. 164.308(b)(1) and C.F.R. 164.502(e)(1) et. seq.
6. 45 C.F.R. 164.314(a)(2)(C)
7. 45 C.F.R. 164.304
8. 45 C.F.R. 164.402
9. 45 C.F.R. 164.404(a) and 164.508(a) et.seq.
10. 45 C.F.R. 164.410 (a)
11. DHHS, Office for Civil Rights: Fact Sheet: Ransomware and HIPAA. 2016. Available at http://bit.ly/2ml8Mgd

by John P. Benson, JD, AHFI, CFE

Telemedicine, Part 2: Navigating the steps to the practice of telehealth care

» Licensure requirements are evolving to streamline the practice of telehealth.
» Telehealth care's exponential growth rate creates a frenzied, reactive regulatory and administrative response.
» Enrollment regulations and policies are in perpetual flux.
» Communication of PHI/PII must be trusted, authenticated, and encrypted for HIPAA compliance.
» Telehealth care creates a powerful convergence of data, knowledge, and technology with a potential for delivering greater efficiencies.

John P. Benson *(john@verisys.com) is Chief Executive Officer and Co-Founder of Verisys Corporation in Alexandria, VA.*

Part 1 of this article appeared in the January 2017 issue of Compliance Today.

Part 1 of this article series covered the origin and drivers of telehealth and telemedicine. In summary, the evolution of telemedicine has been positively demonstrated to improve patient outcomes, lower federal healthcare spending, expand patient access to quality care, manage the unbalanced ratio of limited healthcare providers to an expanding patient population, and reduce hospital ER/ED wait times and loads.

Benson

For the balance of this article, the use of the term *telehealth care* will refer to both telemedicine (the remote experience of clinical healthcare) and telehealth (monitoring, training, and other support mechanisms through a remote protocol). In either case, the web, telephony, secure servers, and apps are in use.

This rapidly expanding platform of healthcare introduces complexities that could implode the hospital administrative system because of the exponential growth of not only the practice of telehealth care, but also the use of locum tenens. As the use of telehealth care evolves, scalability and security will be the prevailing considerations as the massive Baby Boom generation reaches Medicare age.

Foundational concepts

Before we look at the steps that enable the practice of telehealth care, the following paragraphs describe foundational concepts.

Connectivity between providers and patients

Telehealth care enables providers and patients to connect nationwide or globally. Patients can seek and receive care from specialists no matter where the provider chooses to practice, connecting patients with the best providers

for his/her individual conditions without the added time, risk, or expense of travel.

Connectivity between providers and between providers and academics/researchers

Sharing knowledge contributes to higher assurances of favorable outcomes as well as accelerating research by removing the barriers of institutional silos. For those who participate in collectively treating challenging cases and contributing to research, relevant data is correlated to a greater universe and applied more quickly to patients from diverse populations.

Increasing the level of transparency of providers in the system and enhancing consumer choice

Telehealth care and the regulatory requirements of licensing, credentialing, privileging, enrollment, and compliance enhance transparency as providers navigate through the required steps to practice in multiple institutions and states. Although those who have something to hide will likely self-select out and choose not to practice telemedicine for fear of exposure, for those who do participate, the steps create an added gatekeeping layer. Telehealth, being web or app enabled for consumers, will create a level of transparency that will assist in consumer choice—not necessarily referral-based or network-based, but based on the provider with the best credentials, outcomes, and pricing, or a market-driven combination of the three.

Steps to compliant telehealth services

A number of steps are required in order to practice telehealth care: (1) licensing, (2) credentialing, (3) privileging, (4) enrollment, and (5) Health Insurance Portability and Accountability (HIPAA) privacy compliance.

Step 1: Licensing

Obtaining a license to practice medicine is the first step in gatekeeping and making sure that professionals are adequately trained to deliver the services permitted under the scope of their license. Each state's licensing board implements the regulations or administrative codes of its state's legislative action. In order to legally practice medicine in multiple states, providers must be licensed according to the unique laws, regulations, and administrative codes of the respective state medical boards in every state in which they wish to practice. The only regulatory burden imposed on the practice of medicine from a federal level is prescriptive authority (i.e.; the ability to distribute or prescribe controlled substances).

If a specialist desires to extend their practice nationwide via telehealth, the specialist could fork out in excess of $50,000 for license fees and countless hours completing some 35–60 pages of various applications per state. The cumbersome reality of practicing medicine nationwide could hinder practitioners from offering services across multiple state lines; however, there are actions in motion to remedy the time-consuming and tedious process, while preserving competency requirements, compliance, and transparency.

A report published by the Federation of State Medical Boards portrays the variety of laws that affect healthcare licensure. For instance, the medical boards of 48 states, plus the District of Columbia, Puerto Rico, and the Virgin Islands, require that providers of telemedicine be fully licensed in the state in which the patient is located; whereas the medical boards of 15 states issue what is termed a special purpose license, a telemedicine license or certificate, or a license to practice medicine across state lines to providers of telehealth care. The medical boards of four states require

providers to register if he or she wishes to practice across state lines.[1]

A coalition of states have put together a streamlined process for gaining reciprocal licensing that spans state borders. It's called the Interstate Medical Licensure Compact. Currently, 22 states have passed legislation adopting the Compact, and other states are moving the legislation forward.[2] The Compact works to simplify licensure requirements among member states, making it easier for providers to practice in multiple states. The Compact comes to the table with two core ideas: (1) increase access to healthcare for individuals in rural as well as underserved areas; and (2) break down the silos of license status by sharing investigative and disciplinary information, resulting in a reduction of patient harm, risk, and fraud.

Step 2: Credentialing

Credentialing is a process intended to certify a provider's competence by researching all related education, training, experience, competence, and licensure. Depending on the state, the payer, and the institution, providers may likely be required to be credentialed with each hospital in which they practice. The Joint Commission (TJC), DNV GL (a hospital accreditation group), Healthcare Facilities Accreditation Program (HFAP), the National Committee for Quality Assurance (NCQA), the Utilization Review Accreditation Commission (URAC), the Centers for Medicare & Medicaid Services (CMS), and commercial payers have a weigh-in on credentialing requirements. Credentialing may not be mandatory in cases such as with private-pay patients, or consultation where the exchange is between physicians while care of the patient remains with the originating physician, or in an instance where practitioners are not required to be credentialed.[3]

The credentialing process is conducted by the Medical Staff Services office whose team is typically overloaded with its own provider population's processes and requirements. The added workload of credentialing telehealth care providers as well as locum tenens practitioners can be unpredictable and unwieldy. To better understand the varying stages of credentialing, one can look at credentialing as a three-stage process consisting of (1) data collection and verification, (2) review, and (3) recommendation and final action.

The first stage is slowed by duplication of efforts. The task of data collection and verification usually happens in several different departments, information is not shared, and each department within a hospital often uses different data sources as well as its own vendor or staff for primary-source verifications.

The added workload of credentialing telehealth care providers as well as locum tenens practitioners can be unpredictable and unwieldy.

Until the digital paradigm is fully and interchangeably adopted and a central source of locked, verified data informs across multiple departments and institutions, the medical staff services team painstakingly researches, requests, waits, and verifies primary-source static data such as a physician's medical school diploma. As it is, each time a provider requests to be credentialed with an additional hospital, another medical staff officer reaches out—again—to that same medical school for information that has already been provided and verified. And that is only one of a dozen or so items that are static, yet go through the

same primary-source verification process repeatedly.

The other two stages are unique to each hospital and involve department chairs, committees, and the board. Policy, bylaws, and procedure either elongate Stages 2 and 3 into 120 days or more, or compress it to a few days by fine-tuning the process of the credentialing board.

Conceptually, the reason to credential a provider is to protect the patient. This is the process where you would find out if that provider has any exclusions, debarments, or disciplinary actions pending, current, or in the past. This process also verifies education, special training, past practice history, and much more. It is where the Medical Staff Services office vets a provider to granular detail so they don't accidentally hire a non-licensed or unqualified provider, a sex offender, or an identity thief.

The practical reason for credentialing is to be eligible to receive reimbursement from federally funded programs such as Medicare and Medicaid. CMS governs whether hospitals are worthy of receiving reimbursements based on compliance with federal regulatory standards.[4] CMS has approved some standard-setting bodies and organizations to certify a hospital as eligible to receive federal reimbursements. The standards are designed to circle back to quality care and patient safety.

With the emergence of telehealth care, both CMS and some standard-setting bodies have worked to develop credentialing-by-proxy processes where treatment hospitals can communicate with and accept credentialing from the originating-site hospitals. In many cases, this means that smaller hospitals can "borrow" the services of specialists from larger hospitals and accept the credentialing of those larger hospitals without jeopardizing their own standing, as long as a specific set of requirements are met.

The list of requirements provided on the Center for Connected Health Policy's website currently include:

- There must be a written agreement between the two parties;
- The distant-site hospital is a Medicare-participating hospital or telemedicine entity;
- The telehealth provider is privileged at the distant-site hospital;
- A current list of the telehealth provider's privileges is given to the originating-site hospital;
- The telehealth provider holds a license issued or is recognized by the state in which the originating-site hospital is located;
- The originating-site hospital has an internal review of the telehealth provider's performance and provides this information to the distant-site hospital; and
- The originating-site hospital must inform the distant-site hospital of all adverse events and complaints regarding the services provided by the telehealth provider.[5]

This list must also fit within the distant-site hospital's bylaws and policies and provides some abbreviation of a full credentialing process, but still requires engagement from the Medical Staff Services office to verify and execute the requirements.

Step 3: Privileging

In addition to provider credentialing, organizations must perform a process of privileging for their providers. Although providers are often educated and licensed to perform a broad range of procedures and provide a wide variety of services, many providers

specialize their work to a much smaller subset of their possibilities. For this reason, healthcare entities must assess the individual skill set of each provider and approve that provider for the various procedures and services offered by the healthcare entity. Without the "privilege" to perform a specific procedure, a provider who might be fully qualified cannot perform the procedure.

Privileging is informed by CMS guidelines,[6] but the process is created and governed by the policies and bylaws of individual hospitals. Processes could include:

- obtaining primary-source verification from a certifying educational institution,
- referral from a supervising provider who holds the requested privileges,
- direct proctoring among other processes that are particular to the type of environment,
- level of risk,
- specific experience vs. training, and
- other considered circumstances.

As with credentialing, CMS and some standard-setting bodies have released standards to enable a privilege-by-proxy agreement between healthcare entities.

Determining the privileging of a provider is a time-intensive effort that is required for accreditation. As with credentialing, CMS and some standard-setting bodies have released standards to enable a privilege-by-proxy agreement between healthcare entities. By taking advantage of these standards, hospitals can reduce the administrative burden of accessing specialists via telehealth methodologies.[7]

Step 4: Enrollment

Enrollment is a key component to receiving payment, and it has as many faces as the payers, the institutions, and the states one chooses to engage with. Typically, a practitioner will enroll with several dozen insurance payers, and each enrollment process takes several months. Payers can require a different sequence in which a hospital must credential, privilege, and enroll. At times, payer requirements can stack the lead times, making for an unmanageable distance between application and compliant practice, and reimbursement.

In order for Medicaid to reimburse covered services, the engagement of telehealth care in providing those covered services must adhere to the federal requirements of efficiency, economy, and quality of care. States can choose to reimburse for telehealth care services in the same way they reimburse for in-person visits and incorporate the additional details (e.g., a facility fee, the providers at both the distant and originating facilities, equipment, and transmission fees) within their standard submission for reimbursement. If a state bills and seeks reimbursement differently than for in-person visits and care, those states will submit a separate State Plan Amendment (SPA). In both cases, request for reimbursement must stay within the Federal Upper Limits of the Affordable Care Act.[8]

Private payers are not required by federal law to provide coverage for any type of telehealth care, but states may require coverage and payment for certain types of telehealth care.

The Public Health Institute's Center for Connected Health Policy covers telehealth-related laws, regulations, and Medicaid programs for all 50 states plus the District of Columbia and publishes an annual report

called *State Telehealth Laws and Reimbursement Policies*.[9]

In the most recent report released in October 2017, it notes that 48 states, on behalf of Medicaid fee-for-service policies, reimburse for live video but not necessarily store-and-forward or remote patient monitoring. Store-and-forward involves the acquisition of clinical information (e.g., image, sound, or data) that is subsequently forwarded to another site for clinical evaluation. Fifteen states include store-and-forward in their Medicaid program policies, and some are requiring private payers to also cover store-and-forward; 21 states reimburse for remote patient monitoring; and nine state Medicaid programs reimburse for all three with restrictions.

Other significant trends include counting the home as an eligible origination site and allowing a virtual initial visit, thus not requiring an in-person consultation to establish a practitioner relationship with the patient prior to providing telehealth care services. Among the variables that states treat uniquely are the location, type of institution, condition being treated, provider type, and whether it is physician-to-physician or physician-to-patient, among others.

To effectively manage revenue flow and ensure timely coverage and payment, it is recommended to be familiar with each respective state law as well as private and federal payer reimbursement policies for each instance of billing. As regulatory requirements proliferate, it is essential to stay current with laws and recommendations so as to avoid compliance violations and the possibility of making false claims.

Step 5: HIPAA privacy compliance

At large, a hospital's compliance program is designed to ensure that a hospital conforms to state and federal law, state and private payer healthcare requirements, and the internally decided ethical and business policies of a hospital.[10] The compliance item most germane to telehealth care is the Health Insurance Portability and Accountability Act (HIPAA) in the effort to protect a patient's privacy throughout the entire life cycle of a remote communication process. Navigating the path of HIPAA compliance through telehealth technology is a new challenge of providers and institutions engaged in telemedicine.[11]

Of the steps mentioned in this article, compliance is the most complex and robust. Where licensing, credentialing, and privileging occur at periodic intervals, compliance is a requirement for each and every interaction a provider has with a patient, collaborator, vendor, referral, or lab. Telehealth care introduces a wide variety of ways in which providers may unknowingly violate HIPAA through misinterpretation or accidental oversight of compliance regulations in every act of communication, documentation, and storage of protected health information (PHI) as well as personally identifiable information (PII).[12]

For example, simply using a commercially available video-chat service to talk with a patient, or sending a text or email to follow up could cause a breach of HIPAA. How? HIPAA dictates that all PHI must be encrypted and protected so that only very specific persons can access it. This includes maintaining encryption and data control during all phases of the information's life cycle—including storage.

When you send an email, it is housed on a server somewhere. Is that server appropriately encrypted? Ditto with the string of electrons that transmits information for a video chat. That information has to pass through a server on its way between provider and patient computers and could be stored as a backup

along the way. If that server isn't appropriately secured and encrypted, it could be possible to unknowingly transmit PHI via unsecured, HIPAA-noncompliant methods. This is especially true in the case of email or text messages, which patients are likely to store *and view* on servers and platforms without the appropriate security protocols.

One solution is to use a secure messaging platform on the provider's network that creates an encrypted, secure connection between patient and provider, as well as provider and provider, at each contact. In the case of messaging, this typically involves storing all information on the provider's network and granting access to the patient and other providers as needed, effectively restricting the information according to HIPAA and state requirements.

Providers would be compelled to create a secure portal to safely communicate to colleagues, labs, and patients; however, where colleagues, labs, and patients may have relationships with multiple providers, they would have user names and logins for each provider.

The future begs for an anti-competitive platform standard that meets HIPAA compliance as well as each state law, and is engineered with level Tier 3+ security measures. Currently, many telehealth app developers do not consider themselves a covered entity or business associate, and therefore, the app is not subject to HIPAA. Many states have enacted privacy and security laws that would govern the use of an app and make an app subject to oversight by the Federal Trade Commission.

Conclusion

For some time, bringing patient records into an electronic format has been an initiative, but with the advent of telehealth care, the electronic health record (EHR); the electronic medical record (EMR); and now, electronic, secure, web-based provider credentialing/privileging/enrollment profiles may become the industry standard.

Technology plays a large part in each and every aspect. With licensing, credentialing, and privileging, industrywide use of comprehensive, current, accurate data; automation; and secure, centralized records would eliminate the duplication of the same efforts by myriad state boards and hospitals.

Telehealth care provides a wider net of quality healthcare to a broader population and, additionally, creates a convergence of knowledge and data through the use of secure technology. Because of the components that require sharing information, silos are dissolving. The proliferation of relevant data enhances research; informs best practices and education; expands patient access to quality healthcare; provides data points for analytics; quickly exposes those who pose risk to patient care; and detects systemic fraud, waste, and abuse.

1. Federation of State Medical Boards, Telemedicine Policies, Board by Board Overview (a state-by-state summary of requirements to practice telemedicine). Available at http://bit.ly/2G37XiJ
2. Interstate Medical Licensure Compact. Available at http://www.imlcc.org
3. Telehealth Resource Centers: "Credentialing and Licensing." Available at http://bit.ly/2DVU9Vi
4. CMS Quality, Safety &Oversight – Certification and Compliance. Available at http://go.cms.gov/2FHr7cx
5. Center for Connected Health Policy: Credentialing and Privileging (provides suggested guidelines for a proxy process). Available at http://bit.ly/2HMWILF
6. CMS Memorandum to State Survey Agency Directors regarding "Centers for Medicare & Medicaid (CMS) Requirements for Hospital Medical Staff Privileging" November 12, 2004. Available at http://go.cms.gov/2EzIhJH
7. 76 Fed. Reg. 25,550 (May 5, 2011), Medicare and Medicaid Programs: Changes Affecting Hospital and Critical Access Hospital Conditions of Participation: Telemedicine Credentialing and Privileging; Final Rule. Available at http://bit.ly/2nGfqLU
8. Medicaid.gov: Affordable Care Act - Federal Upper Limit. Available at http://bit.ly/2E0c5SD
9. Center for Connected Health Policy, The National Telehealth Policy Resource Center: State Telehealth Laws and Reimbursement Policies, Fall 2017. Available at http://bit.ly/2EBHvvM
10. 63 Fed. Reg. 8,987 (Feb. 23, 1998), Publication of the OIG Compliance Program Guidance for Hospitals. Available at http://1.usa.gov/1cedJaK
11. Telehealth Resource Centers: HIPAA and Telehealth. Available at http://bit.ly/2EDOHHX
12. Health IT.gov: Privacy & Security, Integrating Privacy & Security Into Your Practice. Available at http://bit.ly/2E6VlIT

by Susan L. Walberg, JD, MPA, CHC

The opioid epidemic: What compliance officers should know

» The opioid epidemic is creating a very visible compliance risk for many healthcare providers and organizations.

» Many healthcare professionals don't have a clear understanding of how the many state and federal laws and requirements related to prescribing controlled substances may apply to them.

» A wide range of charges have been filed against opioid prescribers who have violated these laws, including involuntary manslaughter, conspiracy, bribery, and racketeering, which has increased anxiety among providers who treat patients with chronic pain.

» Prescription Drug Monitoring Programs (PDMPs) exist at the state level, and include various monitoring and reporting requirements that compliance professionals and practitioners should be aware of.

» Compliance professionals can provide valuable support to their organizations by gaining an understanding of the complex state and federal requirements and by helping to develop policies, procedures, and education to enhance compliance.

Susan L. Walberg *(swalberg@compliancealacarte.com) is a Principal with Compliance Ala Carte, LLC, in Laurel, MD. She is also the author of* Insider's Guide to Compliance *and an award-winning novel,* Finding Maslow.

It is not news to anyone that the opioid epidemic is a critical public health issue, in addition to being an area of heightened scrutiny by various government agencies and regulators. Due to increased enforcement, physicians and other healthcare providers who prescribe opioid medications to help their patients manage pain are becoming ever more cautious about overprescribing those medications. The concern for prescribers of opioids is legitimate, based on the litany of settlements and government actions against providers/prescribers, pharmacies, and drug companies. The quandary for physicians, of course, is that their first priority is to take care of their patients, which often includes managing chronic pain. The focus of this article will be to provide compliance guidance for physicians and prescribers, although other healthcare players bear risk as well.

Walberg

Many types of providers are impacted by the challenges presented in this public health crisis: family physicians (who are responsible for about half of the opioid pain relievers dispensed),[1] physicians who specialize in pain management, neurologists, orthopedic and other surgeons, hospitals, and pharmacies all have potential exposure in this very visible risk area. Other specialties can be impacted as well, due to patients who see multiple specialists to seek relief from various health problems.

The government's concern relating to the opioid epidemic is twofold. First, of course, is the alarming increase in deaths and health consequences related to opioid misuse and

abuse, which has become a public health crisis and is the subject of countless news programs and other media attention. According to *The New England Journal of Medicine*,[2] the opioid epidemic has claimed more than 300,000 lives since the year 2000 in the United States alone. Secondly, issues of drug diversion, "pill mills," and other illegal activities increase the cost of healthcare drug spending and raise concerns from regulators who investigate healthcare fraud and abuse. Federal agencies focusing on this crisis include Health and Human Services (HHS), the Drug Enforcement Agency (DEA), the Food and Drug Administration (FDA), and the Centers for Disease Control (CDC). At the state level, Medicaid fraud task forces, health departments, law enforcement, and licensing and pharmacy boards all have a role in monitoring the prescribing, use, and abuse of opioids.

Several types of cases have been frequently brought in the battle against the opioid epidemic. The most visible and large-dollar cases involve pharmaceutical companies and off-label or deceptive marketing. Off-label marketing cases typically occur when drug companies market a drug for purposes other than what the FDA approved the drug for. These cases often involve physicians as well, when there are financial benefits provided to prescribers for not only prescribing the drug for the unapproved use, but also for conducting marketing activities for that same drug and unapproved usage. These cases are often significant. Purdue,[3] as only one example, paid a settlement of $600 million for misbranding OxyContin® and misleading physicians and patients about the product's addictive qualities. Cardinal Health[4,5] paid $44 million for violating the Controlled Substances Act, specifically by failing to report suspicious drug orders to the DEA.

Although the size of those settlements is jaw-dropping, the impact of opioid-enforcement cases is not limited to these very large drug companies and healthcare organizations. Individual providers are also subject to scrutiny, which can result in life-altering consequences. A wide array of charges occurs as well. A physician in Reno, Nevada, was charged with involuntary manslaughter for prescribing excess controlled substances. That particular doctor received the attention of the DEA, FBI, ATF, IRS, and various local law enforcement officers as a result of his practices.[6] A hospice nurse pled guilty for being part of a conspiracy to divert controlled substances from patients.[7] Another physician, George Kudmani, was sentenced to 48 months in prison for unlawful distribution of controlled substances and healthcare fraud.[8]

> ...the opioid epidemic has claimed more than 300,000 lives since the year 2000 in the United States alone.

Those are just a sample of many cases. In addition to the many drug diversion and money-laundering settlements and convictions, a variety of cases have been filed under the Anti-Kickback Statute (AKS), where drug companies provide remuneration to physicians for marketing their products for off-label use, as referenced earlier. These cases have brought to light truly dangerous practices. In one case, a powerful pain medication, Subsys, which was approved only for breakthrough cancer pain, was promoted and prescribed for much lesser pain, creating great risk for patients. In that case, the CEO was arrested for fraud, AKS violations, and racketeering charges. Insys Therapeutics, the drug company in this case, allegedly provided

bribes and kickbacks to physicians to promote the use of this powerful drug in non-cancer patients.[9] At least one patient is alleged to have died as a result,[10] due to an adverse reaction, and the prescribing physician lost his license. That case is a recent one and has not been fully resolved.[11]

It is very clear, even from this very brief overview of case types relating to opioids, that the potential consequences to patients, as well as to providers, can be severe and need to be avoided in every way possible. And while the eye-popping cases that make the evening news are usually caused by individuals knowingly making bad decisions for the wrong reasons, it is also possible for well-intentioned providers and organizations to run afoul of the various requirements unintentionally, particularly as the opioid epidemic has become the most talked-about public health issue in the country and politicians, legislators, and public health agencies are reacting to this outcry with increased focus.

Key laws

Compliance professionals need to be aware of the steps necessary to mitigate compliance risk for the providers who prescribe opioids. The volume of practice guidelines, articles, laws, and regulations can be overwhelming and are constantly evolving. There are many applicable state laws and licensure requirements, as well as federal laws that compliance officers should understand. Some of those key laws are summarized below, although this is certainly not the entire universe of applicable requirements and doesn't include the entire gamut of state laws that may be in play.

Prescription Drug Monitoring Programs

A Prescription Drug Monitoring Program (PDMP) is a state-administered set of requirements, including an electronic repository of controlled substances prescribed and dispensed within the state. The state laws dictate what reporting and monitoring/checking are required for these databases. Individuals who have professional reasons to view the data may get access, such as physicians and pharmacists. Because the PDMP is state-run, there is no ability to view all drugs dispensed to a given individual nationwide. Some states are, however, collaborating to share data and are working on overcoming the various challenges of integrating their electronic repositories.

State laws are constantly evolving around the use of the PDMP. Pharmacists and providers may be required to review the database in conjunction with writing or filling prescriptions for opioids and other designated medications. One resource that has information on all state laws is the National Alliance for Model State Drug Laws (NAMSDL). The website for this organization[12] can help compliance professionals get started in identifying applicable state requirements, such as required monitoring, reporting, and continuing education related to controlled substances. Because there is a great deal of variation across states, compliance professionals should do some research and become familiar with the requirements of their states with respect to the PDMP and rules applicable to controlled substances.

The Drug Enforcement Administration

The Drug Enforcement Administration (DEA) is within the Department of Justice and is tasked with ensuring that controlled substances are prescribed, administered, and dispensed for legitimate medical purposes by appropriately registered practitioners. The DEA administers the Controlled Substances Act (CSA), which covers a very broad range of matters relating to controlled substances, including establishing the scheduling of various drugs, prescriber registration

requirements, various controls and record-keeping requirements, and criteria for prescribing.

Providers must have a certificate of registration from the DEA in order to prescribe scheduled drugs. This certificate is separate and apart from the license to practice medicine, which is obtained from state licensing boards. The DEA cooperates with states around CSA issues and enforcement, and the DEA also publishes actions taken against prescribers who violate the CSA, which can be reviewed on their website.

The Food and Drug Administration

The Food and Drug Administration (FDA) also has a significant interest in the opioid crisis. The FDA is responsible for approving new drugs for market, including how drugs are labeled and marketed. The Food, Drug, and Cosmetic Act (FDCA) gives the FDA the authority to oversee the safety of food, drugs, and cosmetics. The FDCA is both civil and criminal, and it is a strict liability statute that has been used to find liability in cases of public safety where there was no intent or even specific knowledge involved. The main area of applicability, for purposes of this article, would be in cases of misbranding or adulteration of drugs. Criminal cases under the FDCA are not common.

Many of the high-dollar cases related to off-label marketing are pursued under the AKS and False Claims Act.

Fraud and abuse laws

Many of the high-dollar cases related to off-label marketing are pursued under the AKS and False Claims Act. Although it is beyond the scope of this article to dive into fraud and abuse laws, it is important for compliance officers to understand that prescribers' relationships with pharmaceutical representatives is an ongoing risk area. Under the AKS, both the party giving the remuneration and the party receiving it may be found liable, and there is no de minimis requirement. Gifts to physicians, such as golf outings and tickets to sporting events, are the more well-known "perks" that have historically been given to physicians in exchange for either prescribing or marketing a given company's drugs. Other financial arrangements bear scrutiny as well, such as drug companies paying physicians for speaking gigs, consulting arrangements, or "preceptorships," where the drug company basically pays the physician to allow the drug representative to shadow the physician. All of these sorts of arrangements have been considered problematic according to the HHS Office of Inspector General (OIG) and should be reviewed. All of this is particularly troublesome when off-label marketing is involved. In the cases where opioids have been the drugs at issue, the potential health consequences to patients have been quite serious. Other fraud and abuse laws have been implicated in some of these cases as well, such as racketeering, money laundering, etc. The main point here is just to provide a general understanding as to the scope of potential laws and consequences that may come into play.

Compliance program implications and recommendations

When you consider that all of the above is a very limited snapshot of the laws and impact of inappropriate opioid prescribing, it is no wonder that physicians are very wary of prescribing opioids. Sadly, this can

lead to under-prescribing in those cases where physicians decide to stay away from prescribing those drugs that could get them on the government's or payer's radar, even when it may be the best alternative for a given patient.

Compliance professionals can assist physicians by helping to identify and establish appropriate processes and safeguards in their practice. Compliance professionals can take some key steps to help implement effective safeguards.

Learn the state's requirements

Identify the expectations and/or requirements of the Prescription Drug Monitoring Program that apply to your physicians/prescribers and your pharmacy (if applicable). Where there are reporting requirements, create a process to streamline that activity as much as possible, and educate the physicians, pharmacists, and staff who need to be involved. Even if PDMP monitoring is not required, it is a good idea to establish a policy for checking the database when the frequency of prescription requests seems excessive or other factors warrant concern. That way, the provider will know if the patient is receiving controlled substances from other providers, which is obviously important information.

Identify a set of protocols for dealing with chronic pain patients

Those protocols should be documented, and steps taken in accordance with those protocols should also be well documented.

- Pain assessment (Pain scale 0–10);
- Review and update list of medications;
- Review patient social history, including substance abuse history;
- Provide treatment alternatives and benefits, including opioid therapy;
- Document treatment decision, goals, and basis for a decision to use opioids (e.g., alternative treatment methods that have failed);
- Examination of pain cause/source;
- Urine drug screen tests (protocols to identify frequency and criteria); and
- Agreement with patient for controlled substance use.

Establish controls or limits for pharmaceutical representative gifts

Prescribers and/or pharmacists should not be accepting gifts and other remuneration from pharmaceutical and device company representatives. Compliance professionals should survey their organization to verify that this is not occurring. Develop policies and procedures to address this risk area.

Review the CMS Open Payments database

Verify that physicians in the facility or practice are not receiving remuneration from drug and device companies that you are not aware of. These relationships can be a red flag for the government, so it's a good idea for the compliance professional to occasionally review this database to ensure there are no surprises.[13]

Create an education module or training session

Physicians and other prescribers should receive training that includes the state and federal requirements related to prescribing and distributing opioids, as well as cases in the news. The training should include the policies and procedures created to address this risk. The training should be

mandatory. (Tip: See if there is a way to get CME credits, which will improve physician cooperation.)

Conclusion

These are some key suggestions to minimize compliance risk for those providers who prescribe controlled substances/opioids. This is obviously a very high-level article, given the variation across states and the multiple laws, regulations, and licensing requirements involved, but hopefully it will give compliance professionals a better understanding of this unique and visible risk area. The opioid epidemic is a national public health crisis, and new laws and regulations will continue being promulgated until this emergency in under control. Compliance professionals can and should have a role to play in protecting their organization's patients, providers, and reputation.

1. American Academy of Family Physicians (AAFP): Chronic Pain Management and Opioid Misuse: A Public Health Concern (position paper), August 31, 2017, citing Daubresse M. Chang HY, Yu Y, et al.: "Ambulatory diagnosis and treatment of nonmalignant pain in the United States, 2000-2010" *Medical Care* 2013;51(10):870-878.
2. Rebecca L. Haffajee and Michelle M. Mello: "Drug Companies' Liability for the Opioid Epidemic" *The New England Journal of Medicine*; December 14, 2017. Available at http://bit.ly/2CxBcrd
3. *United States of America v. The Purdue Frederick Company, Inc.* et al. Available at http://bit.ly/2GYTdl3
4. U.S. Attorney's Office: District of Maryland, press release: "Cardinal Health Agrees to $44 Million Settlement for Alleged Violations of Controlled Substances Act" December 23, 2016. Available at http://bit.ly/2EaWUpQ
5. U.S. Attorney's Office, Southern District of New York, press release: "Manhattan U.S. Attorney Announces $10 Million Civil Penalty Recovery Against New York Pharmaceutical Distributor Kinray, LLC" December 23, 2016. Available at http://bit.ly/2nKkQ9p
6. Ben Margiott and Digital News Staff: "Reno doctor in pill mill case sentenced to 10 years in prison" *News 4-Fox 11*; November 20, 2017. Available at http://bit.ly/2EqLGwW
7. U.S. Attorney's Office District of New Mexico, press release: "Registered Nurse Formerly Employed by Hospice Care Provider Pleads Guilty to Federal Prescription Opioid Conspiracy Charges" June 15, 2017. Available at http://bit.ly/2F55SSR
8. U.S. Attorney's Office: Western District of Kentucky, press release: "Louisville Physician Sentenced to 48 Months in Prison For Unlawful Distribution of Controlled Substances and Health Care Fraud" June 5, 2017, Available at http://bit.ly/2suyhiF
9. Nate Raymond: "North Carolina accuses drugmaker Insys of scheme to push opioid" *Reuters*; December 31, 2017. Available at http://reut.rs/2H1nAay
10. Eric Sagonowsky "Insys's 'reckless' subsys marketing led to patient death, lawsuit alleges" *FiercePharma* March 31, 2017. Available at http://bit.ly/2F4z5Nw
11. U.S. Attorney's Office: District of Massachusetts, press release: "Founder and Owner of Pharmaceutical Company Insys Arrested and Charged with Racketeering" October 26, 2017. Available at http://bit.ly/2j74zfi
12. National Alliance for Model State Drug Laws website: http://NAMSDL.org
13. CMS: Search Open Payments website. Available at http://bit.ly/2C8ClJ1

by Vanessa Pawlak, CHC

Compliance: Digitally streamlined

» Consumerism and value-based care are forcing healthcare organizations to adopt digital technology to increase quality of care and deliver more "on-demand" care while reducing costs.

» The digital transformation in healthcare will create new demands on compliance professionals.

» Compliance professionals must adopt automation tools to protect their organizations by anticipating and addressing emerging issues while minimizing costs.

» Compliance leaders must start conversations with chief information officers about how to automate the areas of routine work and greatest compliance risks.

» Automated compliance processes will be a value-added competitive advantage in a consumer-driven healthcare market.

Vanessa Pawlak *(vanessa.pawlak@cognizant.com) is Global Health Compliance Leader with Cognizant Consulting in South Lyon, MI.*

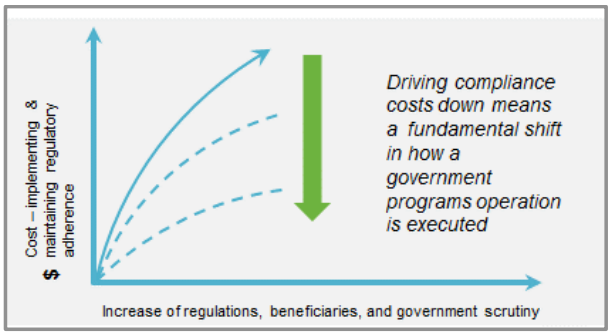
Healthcare organizations today face new competitors, ranging from Amazon and its apparent plans to launch an on-demand healthcare platform to the thousands of venture capital-backed entrepreneurs who want to reshape the industry's delivery models. Then there's pressure to move to value-based care models, which will increasingly drive reimbursements and create new demands on data collection and reporting. Digitally savvy consumers want more convenient and less expensive access to care, augmented by the data they collect on themselves via wearables and smartphone apps.

Pawlak

Compliance professionals won't be insulated from these trends. In fact, we will be called on to provide solutions to the inevitable new regulations that will arise around digital healthcare delivery—and our jobs will be more complex than ever. Checklists and manual processes simply won't be effective compliance tools in complex, multisystem environments that offer digital services ranging from text messaging to virtual consults via smartphone cameras. Traditional compliance methods will be too expensive and ineffective, unable to keep pace with new services and data collection, thus exposing organizations to risk and censure—not just from regulatory agencies, but from healthcare consumers, too.

Fortunately, the same digital technology that is shaking up the industry can help compliance professionals modernize processes to reduce costs, improve efficiency, and even turn compliance operations into a competitive advantage. Compliance operations that use digital tools to automate processes will be more effective at helping their organizations be compliant. Stakeholder satisfaction is an important performance measure for value-based reimbursements, and a compliant organization is more likely to please its members and patients. Further, digitally equipped compliance professionals are better positioned to anticipate and address

Figure 1: The Compliance Cost Curve



emerging risks, and to provide insights their organizations may use to deliver cost-effective, remarkably accurate, and well-managed healthcare. These are reasons why automated compliance operations quickly become a competitive advantage in a complex, highly regulated industry.

Bending the compliance cost curve with automation

As regulations increase, compliance costs go up as well. Automating compliance processes pushes the cost curve down, even as compliance complexity increases (see Figure 1).

Deploying automation effectively, however, requires health compliance leaders to understand what people, processes, and technology they can control, what they can't, and what they may influence. Then they can align implementation efforts accordingly for measurable benefits (see Figure 2). Moving to digital means first understanding where and how you can deliver transformational upgrades.

Digital compliance at work

Once it's understood where digital technologies, specifically automation, can make a difference, compliance officers have powerful tools at their disposal. For instance, the rise in regulatory technology, commonly referred to as "RegTech" in the finance industry, is slowly making its way into the healthcare industry as a form of digital compliance. Automated work flow tools also improve productivity. Software robots (literally lines of computer code) efficiently address data regardless of structure, unlocking new insights and turning faster results. Robotic process automation (RPA) reduces time and effort while improving data collection and reporting accuracy. Software robots in RPA solutions automatically carry out commands, such as collecting and collating data from disparate systems that don't normally communicate. Where it routinely takes long hours and sometimes a dozen people to pull, sort, and synchronize data from multiple systems to prep Medicare and Medicaid contract-level universes, an RPA solution can accomplish those activities, perform dry runs, and test results in a fraction of the time. RPA solutions can also run continuously in the background, identifying non-compliant transactions as they occur so

Figure 2: Aspects of control

Aspect	Description	Degree of authority
Rules and regulations	Government-issued mandates that must be followed	No control
Company infrastructure	Compliance program, people, hardware, the operational environment	Influence
Software and tools	Automation mechanisms customized to meet the needs of the desired element to be monitored or processed	Control

they can be rectified in near real-time versus being discovered months after the fact.

Combining automation tools, RPA, RegTech, machine learning, and artificial intelligence (AI) creates new capabilities that not only make specific compliance tasks easier to accomplish, but also enable compliance officers to rethink how programs and processes are designed. RPA can reduce the cost and fatigue associated with operational audits, with the software "bots" gathering and reconciling data from required systems, streamlining the actual audit process, and freeing compliance and operations professionals to focus on higher value work.

Digital compliance tools and processes also can:

- **Make retroactive corrections easy** with a robot executing huge amounts of work in a tenth of the time a roomful of people would spend addressing backlogs or tedious retroactive file reviews and corrections.
- **Reduce redundancies** and alleviate and resolve discrepancies found across systems.
- **Enable continuous compliance monitoring** to provide real-time audit numbers with monitoring that shows production metrics results against required thresholds.
- **Provide Medicare contract-level metrics** by pulling beneficiary data and their transactions across multiple systems of record.
- **Aggregate Star rating data,[1] HEDIS data,[2] and MACRA data[3]** spread across systems so data that cuts across multiple systems can be seamlessly consolidated and reported.
- **Produce near 100% accuracy on first-pass** yield on health transaction processing.
- **Move compliance** from being built into the rhythm of the business (people and operations) to being built into systems of intelligence (technology and AI) across functions.
- **Meet CMS standards, HITRUST security standards,[4] and NIST standards,[5]** and interact with any user interface.
- **Enable redirection of people and resources** away from repetitive, tedious tasks to other important activities, thus reducing the cost of compliance.

> The annual compliance audit work plan can be an excellent guide to identifying automation opportunities and addressing the greatest compliance risks...

Starting the digital conversation

Getting automation-via-digital underway requires the chief compliance officer (CCO) to open discussions with the organization's chief information officer (CIO) or chief digital officer (CDO), if one exists. These executives should have a sense of the organization's overall digital strategy and where and how addressing compliance automation will augment it. That said, the CCO should be prepared to discuss these key items.

The pain points

Know which processes in the department involve the most manual labor. These usually involve proprietary formats and systems that require workarounds and collating data from different systems, which consumes time and thus money. Identifying the rote, repetitive elements in these processes is work for software bots and/or intelligent workflow automation tools.

Making compliance routine vs. reactive

In the digitally driven health economy, speed is key, and compliance officers increasingly

will be held accountable for anticipating compliance concerns, not just reacting to them. Automating compliance processes so they become routine helps achieve proactive monitoring, with issues caught almost as they occur. Intelligent RPA can even "learn" which transactions are likely to cause issues and flag these so end users take greater care completing them. History can be a guide here: A software bot can monitor for the top three to five compliance issues during claims processing and catch in near real-time, say, a failure to appropriately adjudicate benefits for a special-needs plan member that might cause disruption and possible concerns about access to care. Correcting the error at this stage can help prevent non-compliance, reduce complaints from upset stakeholders, further prevent costs associated with redressing the error weeks after it occurred, and/or reduce its impact on a reimbursement quality measure.

Assessing the highest exposure

The annual compliance audit work plan can be an excellent guide to identifying automation opportunities and addressing the greatest compliance risks, whether defined in volumes or dollar amounts. Once running, software bots can continually monitor these areas, enabling the compliance team to confidently move to the next priority.

Looking ahead

As organizations drive more technology-enabled processes into their operations, an era of cross-industry systems of intelligence will emerge. Although this may seem like a privacy and security risk, blockchain and other data safety enablers will provide the protection required for an entire industry to share data and collaborate in new and exciting ways.

Eventually, health organizations will sync directly into the Centers for Medicare & Medicaid Services (CMS) systems, and real-time numbers will be produced effortlessly as CMS agents and auditors watch regulatory adherence on their compliance dashboard, organization by organization, region by region, and contract by contract. CMS's Health Plan Management System (HPMS) will be a thing of the past. In the future, CMS will monitor compliance digitally through automated means without ever having to knock on the door. The only time the agency will notify a contract sponsor will be to ask why they see a blinking red light on their dashboard over a contract and operation for a measure they care about. As machines learn more and AI enhances human and robotic decision-making, these blinking red lights will be auto-correcting, with end users simply notified there was an issue and how it was resolved. Federal and state governments will then be able to aggregate this information to benchmark compliance with their standards and tie it directly to the health of the population at large.

Health compliance operations that adopt powerful digital tools now to automate compliance processes and procedures will help their organizations thrive in this connected health world. They will bend the compliance cost curve even as they improve adherence to standards designed to provide higher quality of care and drive consumer satisfaction. Finally, compliance professionals will be equipped to take a lead role in value-based reimbursements, healthcare consumer engagement, population health efforts and, ultimately, the viability of the organization itself in an intensely competitive, digitally driven industry. It all begins with digitally streamlining compliance now.

1. CMS press release: (Overall Hospital Quality Star Rating): "CMS updates website to compare hospital quality" December 21, 2017. Available at http://go.cms.gov/2BTHvsp
2. National Committee for Quality Assurance (NCQA): The Healthcare Effectiveness Data and Information Set (HEDIS) and Performance Measurement: Available at http://bit.ly/2lmgQsb
3. CMS.gov: "What's MACRA?" (Medicare Access and CHIP Reauthorization Act of 2015). Available at http://go.cms.gov/1Gb6GDL
4. Health Information Trust Alliance: Introduction to the HITRUST Common Security Framework. 2014. Available at http://bit.ly/2svNsbg
5. National Institute of Standards and Technology (NIST): Computer Security Resource Center. Available at https://csrc.nist.gov/

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)®

- Rachel R. Akins
- Mitchell Baroody
- Jettie Blanton
- Charles P. Braley
- Kathryn S. Burnett
- Paul Colomb
- Solange I. DeLahongrais
- Patricia Ellis
- Nadine Ennever
- Arica Evans
- Dan Eveland
- Margaret A. Fischbach
- Ashley Fleischmann
- Michelle Fountain
- Jenny Lee Garza
- Randal Greene
- Priscilla L. Heeter
- Donny Henry
- Erin K. Hoben
- Aaron Houser
- Kimberly L. Jefferson
- Karen A. Jones
- Rachel M. Kauffman
- Kelly M. Kreiselmeier
- Eddine Luma
- Karyn L. Lushinks
- Pam Matthews
- Matthew R. Mayo
- Michelle B. Moyer
- Victorianne C. Musonza
- Mary Frances Nesbitt
- Fernando A. Nin
- Tim Noonan
- Nathalie Nopakun
- Angela Nunez
- Patricia M. Padurean
- Jan Patterson
- Christina Peterson
- Christopher M. Roane
- Rosie Rutley
- Laurie Shielee
- Autumn Smallwood
- Jeffrey B. Smith
- Lynn Steffes
- Jim Sterling
- Glenda Stewart
- Justin Stone
- Jennifer Tidwell
- Bettina Vanover
- Cassie Villegas

Certified in Healthcare Research Compliance (CHRC)®

- Shannon R. Crites
- Tracy M. Morrison
- Emily Panepinto

Certified in Healthcare Privacy Compliance (CHPC®)

- Flatia L. Addison-Pinellas
- Jonathan D. Avila
- Rona Biele
- Wendy Brazil
- Kristin M. Carpenter
- Elizabeth Cerutti
- David Cook
- Ryan A. Dees
- Pamela Delbridge
- Christopher Dendy
- Jennifer R. Gaede
- Kathleen M. Gingras
- Laura J. Herzog
- Jeanette Jepson
- Keith Lefkowitz
- Connie Madden
- Robert E. Maggs
- Mary C. Malone
- Jennifer Martin
- Jonathan W. McGuire
- Jennifer J. Noren
- Kembrlee S. Potter
- Sandra J. Puka
- Natascha Rowland
- Kathi Samuels
- Derek N. Stoffers
- Christina Trimble
- Jackie Van Cleave

CCB COMPLIANCE CERTIFICATION BOARD

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 compliancecertification.org, or call 888.580.8373.

Want to become

Certified in Healthcare Compliance (CHC)®?

BE RECOGNIZED for your experience and knowledge!

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

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

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

More questions? Email ccb@compliancecertification.org.

Hear from your peers

***Ta-Tanisha Thomas**, MBA, CHC*
Compliance & Ethics Department
American Health Companies, Inc.
Franklin, Tennessee

Why did you decide to get certified?

I was introduced to the healthcare industry during a summer job as the front desk receptionist with Hospice, at the age of 16. Since then, I've worked in behavioral health, hospital system, as well as the continuum of long-term care. Consistently, in each facet of the industry, every organization's goal has been similar—increasing or improving quality while reducing or controlling cost. I believe the junction is where compliance lives, and the reason I sought certification in this area.

How do you feel that having the CHC certification has helped you?

I completed my MBA in healthcare administration in 2011. The compliance certification is an enhancement of that knowledge and serves as a stamp of approval to the recommendations, advice, and direction I share with my colleagues regarding our operational activities, as well as elements to strengthen our compliance program.

Would you recommend that your peers get certified?

I would recommend that my peers get certified because credentials set us apart from the pack, and our professional roles are vital to an organization's success.

CHC™
CERTIFIED IN HEALTHCARE COMPLIANCE

HCCA *welcomes* NEW MEMBERS

ALABAMA
- Judd Harwood, Bradley

ALASKA
- Michael Douglas, SEARHC
- Kyan Olanna, ANTHC
- Holly Torres, South Peninsula Hospital

ARIZONA
- Adam Barker, Banner Health
- Joyce Cox, HealthSplash
- Nicholas Fahlgren
- Zachary Galli, Dignity Health
- Ronald Gishey, Banner Health
- Brenda Hanserd, United Cerebral Palsy of Central Arizona
- Wanda Manuel, Gila River Health Care
- Lisa Moore, Southern Arizona VA Health Care System
- Paul Norman, Touchstone Health Services
- Brian Shannon, Dignity Health

CALIFORNIA
- Brittany Anguiano, Inland Empire Health Plan
- Brian Applegate
- Samantha Bedford, Molina Healthcare, Inc
- April Bernabe, Long Term Care Institute
- Valencia Blackstone, VSP Global
- Melissa Cannon, VSP Global
- Natasha Cogdill, Community Medical Centers
- Margaret Denton, University of the Pacific
- Amber Duong
- Marie Esparza, Community Medical Centers
- Donna Fone, Alameda County Behavioral Health Care Services
- Ryan Galli, Desert Oasis Healthcare
- Mareline Godfrey, University of California-San Diego
- Maria Gregorio, VSP Global
- Carlos Gurley, VSP Global
- Tina Hecht, SnF Management
- Alisha Hightower, Guardian Life of America
- Sage Howard, Gateway Learning Group
- Kellie Jones, The Fox Group
- Edward Kiernan, Marin County Counsel
- Karen Kim, Henry Mayo Newhall Hospital
- Nancee LeeAllen, Front Porch
- Nicole Machado, One Community Health
- Juan Maldonado, Kaiser Permanente
- Jacob Margolis, County of Orange
- Yolanda Morris, St. Joseph Heritage Healthcare
- Scott Olson, Rebekah Children's Services
- Kim Osajda, Gold Coast Health Plan
- Gloria Ruiz, PAMC, LTD
- Frank Russo, Silverado
- Laurie Schrum, Crestwood Behavioral Health, Inc
- Pamela Simpson, Kaiser Permanente
- Mara Sorkin, Visiting Nurse & Hospice Care Santa Barbara
- Dionna Taylor, Northeastern Rural Health Clinics
- Bruce Trevithick, ComRevs, LLC
- Jesse Weldon, Shield HealthCare
- Tracy Whitehurst, Kaiser Permanente
- Anne Wigham, City of Hope
- Carla Williams, Western Health Advantage
- Trina Yen, Kaiser Permanente

COLORADO
- Doris Kirchner, Vail Health
- Lori Pereira, Community Reach Center
- Caroline Wright

FLORIDA
- Jennifer Ambs, Florida Hospital Waterman
- Charles Kizer
- Scott Knowlson, Alliance Physical Therapy Partners
- Maja Lacevic, Trenam Law
- Lisa Rodriguez, Agency for Health Care Admin
- Michael Wellman, HealthyAgile LLC
- Tosha Zimmerman, DaVita Inc

GEORGIA
- Felecia Daniel, Grady Health System
- Sandra Kate Ellington, Meadows Regional Medical Center, Inc
- Lori Foley, PYA, PC
- Jay Harmon, BorderHawk
- Veronique Horne, Emory University
- Grace Kopache
- Anna LaFae, Emory University
- Sabrina LeBeau, Health One Alliance
- Tammy Sanchez
- Carmealla Steele, Grady Health System
- Amy Wamsley, Tenet Healthcare

HAWAII
- Rachael Brant

ILLINOIS
- Shondralis Allen, University of Chicago Medicine
- Amy Beyer, Rush-Copley Medical Center
- Jennifer Clyatt, Heritage Operations Group
- Jessica Cummings
- Cynthia Gibson, Advocate Healthcare
- Francine Lynch
- Daniel Mickleborough, Healthspring
- Michaela Monaghan, Health Care Service Corporation
- Kathryn Patrick, AIM Specialty Health
- Rory Petrisin, HFRI, LLC
- Gretchen Wehrenberg Stewart, Northwest Community Hospital

INDIANA
- Allison DeYoung, Hall Render Killian Health & Lyman, PC
- Deborah Dubeck, Franciscan Alliance
- Nicole Meyer, Indiana Health Centers, Inc
- Adam Oatess, Ascension Health

IOWA
- Corinne Elscott, Wellmark Blue Cross Blue Shield
- Nancy Ruzicka, Mercy Medical Center

KANSAS
- Stacy Jeffress, Kansas Department for Aging & Disability Services
- Janette Kirkpatrick, Lawrence Memorial Hospital
- Kimberly Lynch, Kansas Department for Aging & Disability Services
- Janet Smith

KENTUCKY
- Spencer Kerber, Baptist Health
- David Pearce, Amedisys

LOUISIANA
- Robert Duggan, University of Virginia Physicians Group
- Karen Mai, Lafayette General Health
- Catherine Maraist, Breazeale, Sachse and Wilson, LLP
- Raeni Petry, Gueydan Memorial Guest Home
- Rebecca Prejean, LHC Group, Inc
- Renee Thibodeaux, LHC Group, Inc

MAINE
- Marci Alexander, Maine General Health
- Peter Schleck, Eastern Maine Healthcare Systems

MARYLAND
- Cheraine Christian, University of Maryland Medical System
- Margaret Flanagan, Health Care for the Homeless
- Maegan Jones, The Retina Group of Washington

MASSACHUSETTS
- Helany Baylouny, Steward Health Care System
- Kristin Gallo
- Mary Jane Hanlon, Tufts University
- Susan Marre, Dana-Farber Cancer Institute
- Daniel McGonigle, Fresenius Medical Care North America
- Neal Minahan, American Renal Associate
- Nadia Rahgozar, American Renal Associates

MICHIGAN
- Paula DeBono, Henry Ford Health System
- Susan Headley, Metro Health Hospital
- Pamela Mayer, Beaumont Health
- Jeffrey Smith, U.S. Medical Management
- Ivana Tullett, Michigan Medicine

MINNESOTA
- Rachel Akins, Cass Lake IHS Hospital
- Ashley Erdmann, Prime Therapeutics
- Laura LaDuke, Prime Therapeutics
- Stephanie Pahl, CentraCare Health
- Porsha Reed-Weidner, Prime Therapeutics
- Jessica Wieczorek, Prime Therapeutics

MISSISSIPPI
- Mary Smith, Starkville Orthopedic Clinic
- DeJarnette Trice, Advanced Infusion Solutions

MISSOURI
- Vicki Dhom, SSM Health
- Karen Fischer, BJC HealthCare
- Charissa Hill, BJC HealthCare
- Robert Lampe, Home State Health
- Joseph Price, Cerner Corporation
- Connie Schott, Ozarks Medical Center
- Laurie Wood, Barnes-Jewish Hospital
- Pamela Wood

NEBRASKA
- Charles Funk, Ensign Services Inc

NEVADA
- Lyndollyn Cabantog, Children's Specialty Center of Nevada
- Linda Lilleboe, Carson Valley Medical Center
- Tamara Saldana, Children's Specialty Center of Nevada

NEW HAMPSHIRE
- Shelbe Moore, Dartmouth-Hitchcock

NEW JERSEY
- Kimone Brown, Healthix
- Michael Dawson, Precision Spine, Inc
- Rita Jennings
- Alex LaSalle, Seaview Orthopaedics
- Sharon Lawson-Davis, Holy Name Medical Center

NEW YORK
- Dominique Alexander, Catholic Charities of New York
- Penny Coon, Catholic Charities Community Services
- Robert Creaven, Allied Physicians Group, PLLC
- Michael D'Alessandro, Express Drugs & Surgicals
- Brad Fell, Allied Physicians Group
- Mark Hirschhorn, Essen Health Care
- Robert LaPolt, Bassett Healthcare
- Grant Martin, University of VT Health Network - Elizabethtown Community Hospital
- Michele McGrath, CHS - St. Charles Hospital
- Jonathan Nicholas
- Carol Parjohn, Interfaith Medical Center
- Robert Porr, BDO
- Mica Ruppin, Talkspace
- Ricardo Santiago, Allied Physicians Group, PLLC
- Hope Twum-Ampofo, Healthfirst, Inc
- Nigora Vakhidova, Atlantic Health System

NORTH CAROLINA
- Andrew Abbasi, Ide Management Group, LLC
- Deborah Cade, Public Consulting Group
- Heather Cote, Carolinas Healthcare System
- Josh Fischer, Catasys. Inc
- Danny Fulmer, RHA Health Services
- Bob Kornfeld, EBDS LLC
- Emily Moseley, Strategic Health Law
- Sean Smith, Geriatric Practice Management
- Terri Stacker, Blue Cross and Blue Shield of North Carolina
- Marian Taylor, Womble Bond Dickinson

OHIO
- Lynette Becks, eviCore
- Kimberly Breiding, Vibra Healthcare
- Amy Gross, The University of Toledo
- Adam Kozenko, The Center for Health Affairs
- Peggy O'Donovan, Kindred Healthcare
- Timothy Opsitnick, TCDI
- C'Shalla Parker, University of Toledo
- Stella Wohlgamuth, ProMedica

OKLAHOMA
- Susan Britton, Global Health Inc

OREGON
- Whitney Clark, Oregon Health & Science University
- Ghazal Irfan, Cerner
- Brian Laubscher, Siskiyou Community Health Center
- Pam Matthews, Kaiser Permanente
- Craig Paulsen, Regence Blue Cross
- Bruce Rodgers, Willamette Valley Community Health
- Timshel Tarbet, Cambia Health Solutions
- Dee Williams, RADAR

PENNSYLVANIA
- Renee Abda, Berkeley Research Group
- James Allsman, Tandigm Health
- Susan Berryman
- Faye Betsker, Bethany Village
- Donna Blythe, Sunrise Advantage Plan
- Rita Bowen, MRO Corporation
- Scarlett Denman, OSS Health
- Bernadette Gapinski, Centers for Rehab Services
- Kyle Merkel, Independent Medical Expert Consulting Services, Inc
- Carla Parker, OSS Health
- Jesse Repp
- Bettina Vanover, Cognizant

SOUTH CAROLINA
- Ryan Boggs, DHG LLP
- Pam Doughty, eviCore Healthcare
- Ben Owings, DHG, LLP
- Kathryn Rhoad, Regional Medical Center
- Paula Watford, Nelson Mullins Riley & Scarborough
- Edward White

TENNESSEE
- Heather Bassett, XSOLIS
- Michelle Covington, HCA
- Donald Dally, PerfectServe Inc
- Daneen Davis, Erlanger Health System
- Brittnye Franks, Fast Pace Urgent Care
- Luke Hill, Cookeville Regional Medical Center
- Cynthia HUNT, CIGNA Corporation
- Katrina Orrand, HCA
- Valree Peralta, Compassus

TEXAS
- Douglas Bryant, Inservio3
- Christina Casillas, Cardinal Health
- Lindsay Cates
- Kate Conklin, University of Texas Southwestern Medical Center
- LaTanya Cooks, Regent Care Center
- Chris Corrigan, Springstone
- Tanja Cubit, Ensign Services Inc
- Elizabeth Gonzalez, Austin Radiological Association
- Rhonda Halstead, Val Verde Regional Medical Center
- Xochy Hurtado, Val Verde Regional Medical Center
- Natasha Primus, Ensign Services Inc
- Jordan Raschke, Regent Care Center
- Carol Slovacek, Parkland Health & Hospital System
- Jamie Sorley, Silhol Law
- Randy Steinle, Cyber Trust Alliance
- Denise White, Parkland Health & Hospital System

UTAH
- Kevin Erickson

VIRGINIA
- Wendy Bishop, Centra Health
- Lisa Harmon, OrthoVirginia
- Robert Hedstrom, Horizontech, Inc
- JoAnn Hicks, CHAN Healthcare
- Jenny Keith, Centra Health
- Betsy Mewborn, Centra Health

WASHINGTON
- Wendy Blackwood, Swedish Health Services
- Lisa Brock, Overlake Hospital Med Center
- John Fujii, Matrix Anesthesia LLC
- Laura Grubb, Mason General Hospital
- Laurie Halvorson, University of Washington Medicine Compliance
- Kim Holstein, Western Washington Medical Group
- Alex Meinig, The Vancouver Clinic
- David Smith, Valley Medical Center
- Kelly Wallace, MultiCare Health System
- Jane Yung, University of Washington Medicine Compliance

WEST VIRGINIA
- Jo Ann Rakes, St. Mary's Medical Center
- David Richards, Montgomery General Healthcare Systems

WISCONSIN
- Jessica Davies, Aurora Health Care
- Katie Kickhaver, Aspirus Inc
- Duane Tate, ProHealth Care

DISTRICT OF COLUMBIA
- Lisa Adkins, Children's National Health
- David Blank, Quarles & Brady LLP

PUERTO RICO
- Angel Marrero, MedPharm Services LLC
- Yolanda Perez, Migrant Health Center, Inc
- Zabdy Reyes Milliam, MC-21 Corporation

Socialize!

Connect with us and your compliance colleagues on all of your favorite social media platforms.

Join the compliance conversation and help grow the compliance community.

hcca-info.org/
hccanet

facebook.com/
HCCA

twitter.com/
theHCCA

bit.ly/LIGroupHCCA
bit.ly/LinkedInHCCA

youtube.com/
compliancevideos

pinterest.com/
theHCCA

instagram.com/
theHCCA

hcca-info.org/
google

complianceandethics.org

complianceandethics.org/
category/podcasts

Takeaways

April 2018

Compliance TODAY

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

New resolution opportunities in the Medicare appeals process

by Andrew B. Wachler and Erin Diesel Roumayah (page 23)

- The Office of Medicare Hearings and Appeals' (OMHA's) appeal backlog continues to burden the appeals process and healthcare providers and suppliers.
- OMHA and CMS have demonstrated commitment to alleviating the backlog through releasing new and revised alternative dispute resolution (ADR) processes.
- The Low Volume Appeals (LVA) settlement and expanded Settlement Conference Facilitation (SCF) program collectively cover nearly every appeal under $100,000 that was pending with the Administrative Law Judge (ALJ) or Council levels as of November 3, 2017.
- The expanded SCF program, in conjunction with the LVA settlement, has the potential to collectively resolve a large volume of the appeals backlog.
- Medicare-participating healthcare providers and suppliers should continue to expect updates and expansions to existing ADR programs and the release of new programs until the backlog's growth has plateaued and/or the backlog is resolved.

Passing the HCC Audit: What you need to know

by Lisa Knowles (page 31)

- Diagnosis codes are based on the ICD-10-CM guidelines for the current fiscal year.
- Medical record documentation is key and must support the code assignment.
- Each face-to-face encounter must have a valid signature.
- A valid date of service must be on the documentation for each face-to-face encounter.
- Addendums are valid if based on an observation on the date of service.

A sharpened focus on remediation in federal investigations

by Precious M. Gittens and Brett Moodie (page 37)

- Recent DOJ fraud enforcement trends reveal prosecutors' heightened focus on corporate remediation.
- Remediation is a critical factor in DOJ decision-making in criminal and civil False Claims Act resolutions.
- The DOJ has demonstrated that it will scrutinize an organization's internal reaction to allegations of wrongdoing while it is under investigation.
- Remediation can be of enormous value to organizations seeking "cooperation credit" in both civil and criminal matters.
- Organizations that form a multidisciplinary team to oversee internal investigations and remedial actions may be best-positioned to respond to a government investigation or enforcement action.

Board responsibility for compliance oversight and program effectiveness

by Gabriel L. Imperato and Anne Novick Branan (page 43)

- Board should ensure adequate reporting methods for duty of care, decision-making, and compliance oversight.
- Board must address compliance program resources, structure, and operation.
- Board oversight must focus on compliance program effectiveness.
- Board should have access to healthcare compliance expertise.
- Board should have active and ongoing dialog with compliance professionals and strive to promote an ethical culture in the organization.

Ban the Box: A brief overview of criminal background checks

by Andrew Amari and Cornelia M. Dorfschmid (page 50)

- Ban-the-Box (BTB) laws exist at the state, city, and county levels with jurisdictional differences.
- Compliance officers need to understand BTB laws' significance for sanction screening.
- Working with HR to assess BTB laws' potential impact is crucial.
- Careful attention to exceptions for healthcare positions is advised.
- Hiring processes must be compliant with BTB.

Strengthen compliance to avoid management's liability for opioid diversion

by R. Stephen Stigall (page 56)

- The government may turn to the Responsible Corporate Officer (RCO) doctrine to prosecute health system executives for failure to detect opioid diversion.
- Under the RCO, management can be held criminally liable for their subordinates' violations of the federal Food, Drug, and Cosmetic Act (FDCA).
- Making disclosures about individuals responsible for diversion as required to earn "cooperation credit" with the DOJ creates a dilemma for management in light of the RCO doctrine.
- In February 2017, the DOJ released compliance program guidance that provides resolution to the dilemma.
- Bolstering compliance to detect and prevent diversion should preclude charges on a RCO prosecution theory

Data breach compliance after Uber: Avoiding scandal

by Bethany A. Corbin (page 62)

- Data breaches are inevitable, but compliance responses can mitigate damage.
- Breach notification alone should not drive the investigation process.
- Inventory your sensitive data to identify system vulnerabilities.
- Incident response plans can lead to effective breach response strategies.
- Breach validation and containment are crucial to mitigation.

Business associates: Have you really integrated them into your risk profile?

by Marti Arvin (page 67)

- When applicable, business associate agreements (BAA) that meet all of the regulatory requirements must be in place.
- Having an appropriate BAA does not necessarily mitigate the risk for the covered entity.
- The BAA should require the associate to notify the covered entity of incidents that involve a violation of the HIPAA Privacy or Security Rules.
- Covered entities should determine if a business associate's data compromise is a breach.
- Covered entities must exercise ongoing due diligence for business associate compliance.

Telemedicine, Part 2: Navigating the steps to the practice of telehealth care

by John P. Benson (page 71)

- Licensure requirements are evolving to streamline the practice of telehealth.
- Telehealth care's exponential growth rate creates a frenzied, reactive regulatory and administrative response.
- Enrollment regulations and policies are in perpetual flux.
- Communication of PHI/PII must be trusted, authenticated, and encrypted for HIPAA compliance.
- Telehealth care creates a powerful convergence of data, knowledge, and technology with a potential for delivering greater efficiencies

The opioid epidemic: What compliance officers should know

by Susan L. Walberg (page 78)

- The opioid epidemic is creating a very visible compliance risk for many healthcare providers and organizations.
- Many healthcare professionals don't have a clear understanding of how the many state and federal laws and requirements related to prescribing controlled substances may apply to them.
- A wide range of charges have been filed against opioid prescribers who have violated these laws, including involuntary manslaughter, conspiracy, bribery, and racketeering, which has increased anxiety among providers who treat patients with chronic pain.
- Prescription Drug Monitoring Programs (PDMPs) exist at the state level, and include various monitoring and reporting requirements that compliance professionals and practitioners should be aware of.
- Compliance professionals can provide valuable support to their organizations by gaining an understanding of the complex state and federal requirements and by helping to develop policies, procedures, and education to enhance compliance.

Compliance: Digitally streamlined

by Vanessa Pawlak (page 84)

- Consumerism and value-based care are forcing healthcare organizations to adopt digital technology to increase quality of care and deliver more "on-demand" care while reducing costs.
- The digital transformation in healthcare will create new demands on compliance professionals.
- Compliance professionals must adopt automation tools to protect their organizations by anticipating and addressing emerging issues while minimizing costs.
- Compliance leaders must start conversations with chief information officers about how to automate the areas of routine work and greatest compliance risks.
- Automated compliance processes will be a value-added competitive advantage in a consumer-driven healthcare market.

HCCA'S UPCOMING EVENTS

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

April 2018

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
1	2 WEB CONFERENCE: *Fundraising & Patient Privacy*	3	4	5	6	7
8	9 **BASIC COMPLIANCE ACADEMY** Chicago, IL	10	11	12 CHC Exam	13	14
15 **2018 COMPLIANCE INSTITUTE** Las Vegas, NV	16	17 CHC,CHRC & CHPC Exam	18	19 WEB CONFERENCE: *How Effective Is Our Compliance Program? A Case Study in Semi-Structured Interviews*	20	21
22	23	24 WEB CONFERENCE: *Paying Employed Physicians to Supervise Advanced Practice Clinicians*	25	26	27 **REGIONAL CONFERENCE** New Orleans, LA	28
29	30 WEB CONFERENCE: *HIPAA & The Medical Practice: Requirements for Privacy, Security and Breach Notification*	1	2	3	4	5

May 2018

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
29	30	1 WEB CONFERENCE: *Advancing Compliance Efforts through Information Governance*	2	3 WEB CONFERENCE: *Background Screening: What You Don't Know Can Hurt Your Organization*	4 **REGIONAL CONFERENCE** Columbus, OH	5
6	7 **BASIC COMPLIANCE ACADEMY** Anaheim, CA	8	9	10 CHC Exam	11 **REGIONAL CONFERENCE** New York, NY	12
13	14 **BASIC COMPLIANCE ACADEMY** Boston, MA	15	16	17 **REGIONAL CONFERENCE** San Juan, PR CHC Exam	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2

REGIONAL CONFERENCES

April 27 · New Orleans, LA
May 4 · Columbus, OH
May 11 · New York, NY
May 17–18 · San Juan, PR
June 1 · Philadelphia, PA
June 8 · Seattle, WA
June 15 · Orange County, CA
September 7 · Boston, MA
September 14 · Minneapolis, MN
September 21 · Kansas City, MO
September 28 · Indianapolis, IN
October 5 · Pittsburgh, PA
October 11–12 · Honolulu, HI
October 19 · Denver, CO
October 26 · Chicago, IL
November 2 · Louisville, KY
November 9 · Scottsdale, AZ
November 16 · Nashville, TN
November 30 · San Francisco, CA
December 7 · Houston, TX

BASIC COMPLIANCE ACADEMIES

April 9–12 · Chicago, IL
May 7–10 · Anaheim, CA
June 11–14 · Scottsdale, AZ
July 23–26 · Seattle, WA
August 6–9 · Washington, DC
September 10–13 · Las Vegas, NV
October 1–4 · Dallas, TX
October 15–18 · Nashville, TN
November 12–15 · San Diego, CA
December 3–6 · Orlando, FL
December 10–13 · Orlando, FL

HEALTHCARE PRIVACY BASIC COMPLIANCE ACADEMIES

July 23–26 · Seattle, WA
October 15–18 · Nashville, TN
December 3–6 · Orlando, FL

RESEARCH BASIC COMPLIANCE ACADEMIES

December 3–6 · Orlando, FL

22ND ANNUAL COMPLIANCE INSTITUTE

April 15–18 · Las Vegas, NV

RESEARCH COMPLIANCE CONFERENCE

June 3–6 · Austin, TX

Dates and locations are subject to change.

Zebu Compliance Solutions

ZebuCompliance.com • support@zebucompliance.com • 888.395.9029

Why Choose Zebu Compliance Solutions?

Because healthcare needs solutions. Health spending is approaching 20% of GDP, with outcomes in the bottom 20% of developed countries. Fraud, abuse, carelessly wasted resources and redundant paperwork burn almost half of our healthcare dollars with an ROI of ZERO.

Yes, Zebu will save you time. We'll save you hassle. We'll save you from compliance mistakes. We might even save your bacon in an audit. But our bottom line is about our nationally shared bottom line. About spending the right dollars for the right care. About delivering care not because there is something we could do to the patient, but because there's a right thing we should do for the patient. And we want to help you do those things, profitably, and for all the right reasons.

Healthcare done right is justice for everyone: providers, payers, and most importantly, patients. We're passionate about making a difference, and look forward to making a difference with you.

– Francesca Hartop, Founder/CEO

ClaimScrub™

Medical claims done right.

Full verification of correct coding and coverage for claims. Supports pre-service, post-service, and audit implementations.

- Inpatient, Outpatient, Specialty Claim Support
- Plan-specific coverage rules
- Update daily by certified coders using original sources
- Custom Edit Engine
- Historical Edit Module
- Bundling, 3-day rule, post-op periods, related care, duplicate billing, split claims
- Medicare reference pricing
- Payment Calculation for RVUs and Fee Schedules
- Patient Pre-Service Share of Cost Estimations

EPStaffCheck™

Your provider panel: Be the first to know.

Monitor your provider panel, as well as staff and vendors, for exclusion, licensing, and disciplinary status with Medicare, Medicaid, OIG, State, NPDB and regulatory boards.

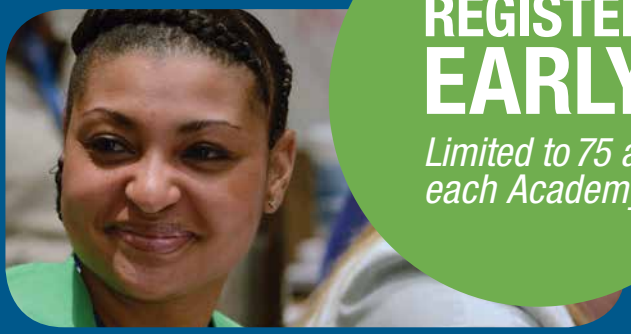
- Sanctions and Exclusions
- Malpractice settlements
- State Board licensing and disciplinary status
- License renewal reminders
- Social Security Death Index (SSDI)
- Open Payments Records
- Medicare Opt-Out Status
- Auditor-Approved Documentation Trail
- Monthly and Annual Management Reports
- Plus:Enhanced Service for Third-Party Accountability

HCCA

Healthcare Basic Compliance Academies

REGISTER EARLY
Limited to 75 at each Academy

- SOLD OUT — April 9–12, 2018 • Chicago, IL
- SOLD OUT — May 7–10, 2018 • Anaheim, CA
- LIMITED SEATS — May 14–17, 2018 • Boston, MA
- LIMITED SEATS — June 11–14, 2018 • Scottsdale, AZ
- July 23–26, 2018 • Seattle, WA
- August 6–9, 2018 • Washington, DC
- September 10–13, 2018 • Las Vegas, NV
- October 1–4, 2018 • Dallas, TX
- October 15–18, 2018 • Nashville, TN
- November 12–15, 2018 • San Diego, CA
- December 3–6, 2018 • Orlando, FL
- December 10–13, 2018 • Orlando, FL



hcca-info.org/academies

Questions: *jennifer.parrucci@corporatecompliance.org*

Want to become Certified in Healthcare Compliance (CHC)®? Apply to take the optional CHC exam on the last day of the Academy.