A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

COMPLIANCE TODAY

MAGAZINE

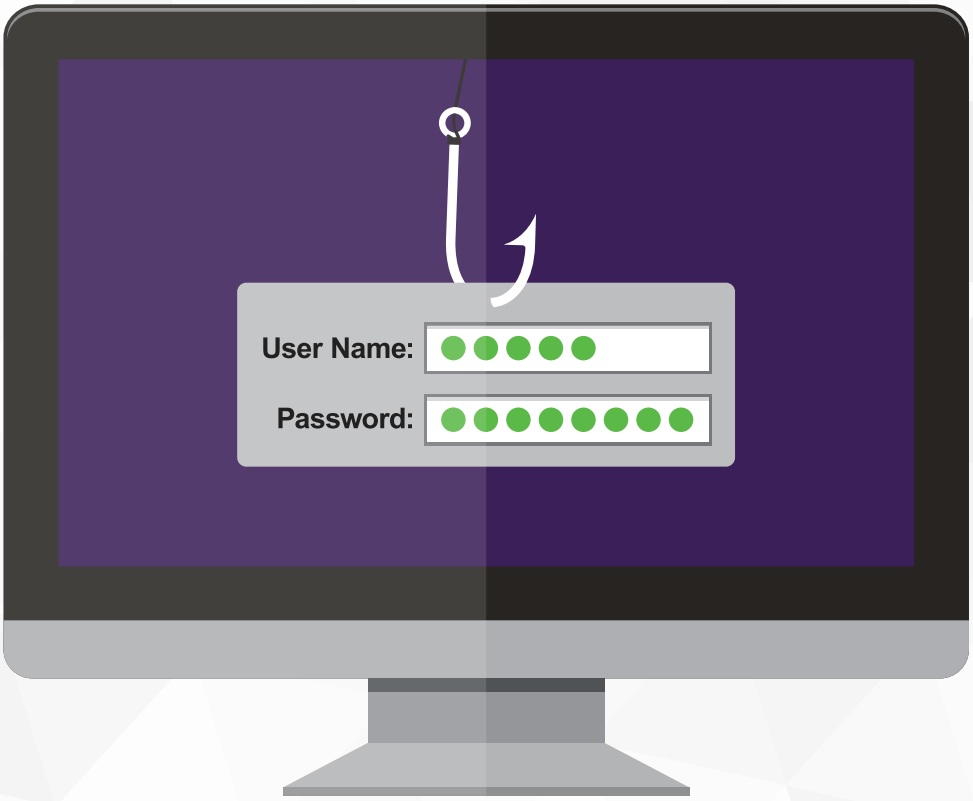
JANUARY 2019

GREG RADINSKY
SENIOR VICE PRESIDENT &
CHIEF CORPORATE COMPLIANCE OFFICER
NORTHWELL HEALTH

SEEING ENFORCEMENT ISSUES FROM ALL SIDES
(P12)

HCCA™

Will Your Organization be the Catch of the Day?



Phishing attacks are on the rise and your employees are the first line of defense. Are you confident they are prepared?

Through a combination of simulated phishing attacks and automatically assigned training, the Phishing Simulator, brought to you by HCCS in partnership with MediaPRO, empowers employees to recognize costly malicious attacks—ensuring your organization is the one that got away.

Stress Less. Care More.
hccs.com/Phishing

hccs
A HealthStream® Company

Which certification should I get next?

by Gerry Zack

I recently noticed someone on LinkedIn who listed 59 certifications—that's right, 59! My first thought was to ask for a business card, just to see how 59 certifications could all be included on a single card, maybe a very large card.

But this reminded me of a question I've received on numerous occasions over the years: "Which should be my next certification?" The answer, of course, is the often-used, "It depends." What it depends upon mostly is your current and anticipated future roles. Let's start with an easy one. You are already certified as a CHC, but you find yourself more and more dealing with privacy issues, or the job you have your eye on would broaden your scope to include research issues. Adding the CHPC or CHRC credential makes the most sense.

But given the broad range of issues that compliance professionals touch on, considering other certifications can also make sense. The Certified Internal Auditor and Certified Fraud Examiner credential each offer opportunities to broaden one's skills to include things that might be complementary to your primary duties, or that could help in one of the areas you already have responsibility for, such as auditing and monitoring or performing certain types of investigations.

So, think first about your current and direct responsibilities, then about complementary or indirect skills, and finally about future needs associated with promotions.

But once you get beyond the scope of HCCA's certifications (offered through the Compliance Certification Board), you quickly realize there are often multiple certifications available that all focus on the same thing. How do you choose among them?

Here are my thoughts on how to pick the best certifications. First, always be wary of certifications that offer waivers of the examination, ones that say that if you have certain experience you won't have to take an exam. They just want your money for a piece of paper. I always say that if you have a lot of experience, the exam should be easier for you, so go take it. Likewise, if no examination is even required for anyone, don't bother. There should always be a clear and objective measure of an individual's knowledge to show they are qualified to hold a credential.

Next, look at the exam itself. How much effort was put into the development (and the ongoing maintenance) of the exam. Organizations like HCCA put millions of dollars into the exam development, and continue to devote significant human and financial resources to keeping the exam at a high level of quality. If all you have to do is skim through a booklet for a couple of hours to pass an exam, the certification is probably not worth it.

The bottom line is that you want a certification that is relevant to your career, but also one that challenges you. CT

Gerry Zack
CCEP, CFE, CIA
Please feel free to contact me anytime to share your thoughts
+1 612.357.1544 (Cell)
+1 952.567.6215 (Direct)
gerry.zack@corporatecompliance.org
@Gerry_Zack
/in/gerryzack/

COMPLIANCE TODAY
A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

January 2019

Features

Columns

Departments

HCCA™
Health Care Compliance Association

888.580.8373 | hcca-info.org

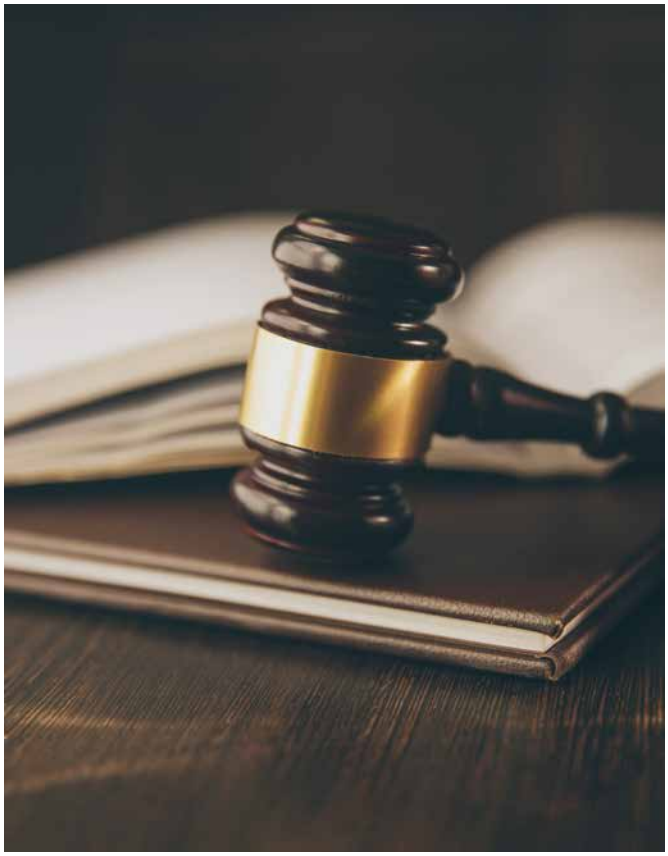
VOLUME 21, ISSUE 1

Articles

Compliance Today is printed with 100% soy-based, water-soluble 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).

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.

Justice Department releases memorandum on litigation guidelines for Civil Consent Decrees and Settlement Agreements



One of the last actions former U.S. Attorney General Jeff Sessions took was to sign a memorandum providing direction to all civil litigating components and United States Attorneys' Offices (USAOs) on the principles that should be followed when resolving a civil lawsuit against a state or local governmental entity. According to the government press release, "State and local governments have unique roles under the Constitution, and the Department is committed to ensuring that its practices in these cases are transparent, impartial, and consistent with fundamental constitutional principles, including democratic control and accountability.

The memo includes guidelines on:

- How civil litigating components and USAOs should handle investigations and reports of allegations;
- The notice, approval, and substantive requirements for consent decrees and settlement agreements, as well as constitutional and policy considerations;
- Use and limits of monitors for state and local governmental entities.

"These guidelines are designed to ensure that consent decrees with state and local governments are narrowly tailored to remedy the alleged violations, and are not used to extract greater relief from the state or local government than the Department could obtain through litigation. They are also structured to ensure that, where appropriate, responsibility is returned to democratically accountable state and local institutions. Requirements include, but are not limited to, limits on duration of a consent decree, clear triggers for termination, and prohibitions on using consent decrees to achieve general policy goals. The memo also clarifies the approval process for both consent decrees and settlement agreements, to ensure that they receive appropriate review by the Office of the Deputy Attorney General, the Associate Attorney General, and other senior Department leadership."

According to Attorney Gabriel Imperato, Managing Partner in the Fort Lauderdale office of Nelson Mullins, "This directive is intended to narrow the scope and effect of consent decrees and settlement agreements and avoid overreaching requirements, especially if it may compromise local control and accountability. The content of the policy suggests limitations on the duration of these types of agreements with state and local government entities and features such as appointment of monitors and onerous reporting requirements to Federal agencies," says Imperato. "As with any policy announcement involving Federal government litigation it remains to be seen what effect this memorandum will have from case to case."

Full text of Sessions Memo *https://bit.ly/2zXSBJz*

Deloitte: Despite supply chain financial crime rates holding steady, just 15 percent tap blockchain to help mitigate risk

An October 2018 survey by Deloitte finds, "During the past five years, an average of 31.1 percent of respondents to annual Deloitte polls say their organizations have experienced supply chain financial crime—particularly fraud, waste or abuse—in the preceding year." CT

For more: *https://bit.ly/2FrnL22*

Regulatory News

OCR and ONC update Security Risk Assessment (SRA) Tool

In October 2018, Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC) and the Office for Civil Rights (OCR) announced they had updated the popular Security Risk Assessment (SRA) Tool to make it easier to use and apply more broadly to the risks to health information. The tool is designed for use by small to medium-sized health care practices (those with one to 10 health care providers, covered entities, and business associates) to help them identify risks and vulnerabilities to electronic protected health information (ePHI).

According to the HHS press release, "An enterprise-wide risk analysis is not only a requirement of the HIPAA Security Rule, it is also an important process to help healthcare organizations understand their security posture to prevent costly data breaches. What is an enterprise-wide risk analysis? It is a robust review and analysis of the risks to the confidentiality, integrity, and availability of electronic health information—across all lines of business, in all facilities, and in all locations."

The press release noted, "ONC and OCR conducted comprehensive usability testing of the SRA tool (version 2.0) with healthcare practice managers. Analysis of the findings across the user base informed the development of the content and the requirements for the SRA Tool 3.0. ONC and OCR then conducted testing of the SRA Tool 3.0 to compare the user experience in completing the same tasks presented in the first round of testing. You'll find the tool to be more user friendly, with helpful new features such as:

- Enhanced user interface
- Modular workflow with question branching logic
- Custom assessment logic
- Progress tracker
- Improved threats & vulnerabilities rating
- Detailed reports
- Business associate and asset tracking
- Overall improvement of the user experience.

"Using a Windows operating system? Download the Windows version of the tool at *https://bit.ly/2BcBtBC*. The iOS iPad version was not updated, but the previous version is available at the Apple App Store exit disclaimer icon (search under 'HHS SRA Tool').

"And don't forget to explore the SRA Tool's website, which provides a revised User Guide to help you get started.

"Remember: All HIPAA covered entities and business associates are required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by their organization. If you haven't conducted a recent enterprise-wide risk analysis, now is the time to download the HHS SRA Tool to help with this foundational element upon which the security activities necessary to protect ePHI are built." CT

For more: *https//bit.ly/2tAo5lP*

Board & Audit Committee Compliance Conference

February 18-19, 2019 | Scottsdale, AZ

New for 2019:

- *Two full days of education and networking*
- *Two learning tracks: General Organizational Compliance and Healthcare Compliance*
- *New location at The Scottsdale Resort at McCormick Ranch*

Buy one registration for $995 and get one for $695

Learn the latest topics in compliance and regulatory risk, including how to best fulfill your fiduciary obligation, oversee financial reporting, and conduct internal audits. This is a great opportunity for board members, audit or compliance committee members, and senior-level leaders to improve the overall compliance performance of their organizations.

hcca-info.org/audit

Questions? *jill.burke@corporatecompliance.org*

HCCA™ Health Care Compliance Association

HCCA Conference News

Board & Audit Committee Compliance Conference

February 18-19, 2019 | Scottsdale, AZ
hcca.org/audit

It is vital for board members, audit committee members, and senior-level leaders to obtain the knowledge and skills they need for better compliance oversight. The Board & Audit Committee Compliance Conference can help leaders to meet these expectations.

This year's conference combines the efforts of the Health Care Compliance Association (HCCA) and the Society of Corporate Compliance and Ethics (SCCE) and features two learning tracks: General Organizational Compliance and Healthcare Compliance. Attendees can take breakout sessions from either track.

During the two-day conference, attendees will learn:

- How to fulfill fiduciary obligations as board/committee members and senior-level leaders
- How to help improve board performance for compliance oversight
- The latest on regulatory risk and compliance obligations
- Tips for successful oversight of financial reporting
- How to conduct internal audits and investigations
- How to improve overall compliance program performance at their organizations

In addition to meeting learning objectives, conference attendees will have ample time for networking at the receptions and during session breaks.

For more information and to register, visit *hcca.org/audit*. Invite a colleague and get the second registration for the discounted rate of $695. CT

Healthcare
Basic Compliance Academies

2019

Orlando • Jan 21–24 SOLD OUT

Scottsdale • Feb 4–7 LIMITED SEATS

Chicago • Mar 18–21

San Diego • Apr 15–18

Minneapolis • May 13–16

Washington DC • Jun 3–6

New Orleans • Jun 17–20

Denver • Jul 22–25

New York • Aug 5–8

Charleston • Aug 12–15

Indianapolis • Sep 9–12

Anaheim • Sep 30–Oct 3

Orlando • Oct 21–24

Las Vegas • Nov 18–21

Houston • Dec 2–5

Nashville • Dec 16–19

Building or expanding an effective healthcare compliance program starts with understanding the fundamentals. During this three-and-a-half-day academy, you'll get to the heart of a basic compliance program, learn from industry experts, and meet other compliance professionals with real-world experiences to share. Participation is limited to 75 participants, so register early — academies fill fast. The optional Certified in Healthcare Compliance (CHC)® exam is offered on the last day.
Separate application and fee required.

hcca-info.org/academies

Questions? jennifer.parrucci@corporatecompliance.org

HCCA™
Health Care Compliance Association

The very heart of the matter: How having open heart surgery reminded me why ethical cultures are so important to an organization and why what I do as an ethics practitioner matters so much

Ann D. E. Fraser
PhD
Executive Director
Values, Integrity and Conflict Resolution Directorate
Canadian Food Inspection Agency

I woke up early the morning of March 15, 2017 with the intention of catching a flight to Moncton, New Brunswick to provide values and ethics training to some of our Agency employees.

When I got up, I knew something was very wrong. I couldn't catch my breath at all. I remembered a quote from Shakespeare's Julius Caesar: "Beware the Ides of March". I didn't ignore what was happening (which was ultimately critical to resolving my dilemma) and I got a colleague to take me to the local hospital emergency and not the airport. This is no different, really, than when we become aware that something is not right within our organization and immediately do something to address it; timeliness is so important.

By the time I reached the emergency department I was breathing more easily and actually didn't feel too, too bad. I hadn't had a heart attack as the blood work and other tests confirmed. In fact all was good. However, you don't, or shouldn't, ignore clear warning signs that something isn't right, so the doctor ordered a chest x-ray. She found my lungs were filled with fluid. "Congestive heart failure" was the term used, but the big question was what had caused it?

Congestive heart failure can be caused by a number of things and may be treated in a number of different ways: life style changes, medications, perhaps a combination of both or, in my case, by valve replacement. It turns out I had a life-threatening

condition—two faulty heart valves. Who knew?!? However, it was taking the time to do the "deep dive"—to determine what the risk and its cause(s) were and then managing them appropriately—that actually saved my life. It was important to understand the root cause.

This is the very reason we carry out, or should carry out, periodic ethical risk analyses/profiles within our organizations. We need to know what our ethical risks are and manage them appropriately to maintain our ethical culture. The first step of an ethical risk analysis/profile is to ask the right questions of employees and examine any prior information we may have to identify the risks we face as an organization. We then carry out a risk validation and assessment to determine what processes we need to put in place to protect the ethical culture of our organization by minimizing/addressing these risks.

I also remember speaking with the anesthetist prior to my surgery and commenting to him that I was a high-risk patient because of my obesity. He smiled at me and said I was not. With the support of my doctors, my blood pressure and diabetes were well controlled and most of me, internally, was in pretty good shape. The doctor's role is not unlike the role that ethics practitioners like me play within our organizations to ensure the organization's "ethical health." For example, by ensuring that employees know what is expected of them in terms of decision-making and behaviors through training, codes of conduct, policies, our leaders, and the like.

I learned too that your condition before surgery also impacts your recovery afterwards. That is to say, the better your physical health, the better and faster your recovery. It's one of the identified advantages of being an ethical organization as well. When dealing with an ethical breach, the healthier the culture, the speedier the return to normal for the organization and the lesser the impact on employee morale.

Recovery from surgery also depends on following the many rules set for you, especially the rule to avoid lifting anything heavy or putting pressure on your arms to push or pull yourself out of bed or a chair. This is to protect the chest bone which was cut to access the heart and now needs to heal. This is no different than following the many rules set out in our codes of conduct and other policies that ensure all employees at all levels make appropriate decisions and behave appropriately in order to maintain public confidence and trust in our organizations.

Three months later and I was back at work as the Agency's ethics practitioner. I now know from my own personal experience that, as an organization, with our Agency`s values, code of conduct, conflict of interest policy, harassment prevention policy, ethical risk profiling work, ethical climate surveys etc. we really are on the right track to ensuring continued ethical health. This is indeed the very heart of our matter. CT

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

PEOPLE *on the* MOVE

WHERE'S YOUR CAREER TAKING YOU?

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.

To submit your news, email
margaret.dragon@corporatecompliance.org

- **Jared M. Barnes**, JD, CHC has been appointed Assistant Legal Counsel at Beth Israel Deaconess Medical Center in Boston.

- St. Luke's Health Care System in Duluth, MN has appointed **Katherine Becker** Vice President of Corporate Compliance.

- Coker Group, with offices in Alpharetta, GA and Charlotte, NC, recently hired **Rosalind "Roz" Cordini**, JD, MSN, RN, CHC as Senior Vice President/Director of Compliance Services.

- **Cindy Hart** has been named Associate Consultant at Acevedo Consulting Inc. in Delray Beach, FL.

- **Jessica Lin**, CHC, CPC has been named Corporate Compliance Manager at El Camino Hospital in Mountain View, CA.

- **Jeff White**, CHC has been named Compliance Officer at Treasure Coast Hospice in Stuart and Fort Pierce, FL.

SEEING ENFORCEMENT ISSUES FROM ALL SIDES

Meet Greg Radinsky

Senior Vice President & Chief Corporate Compliance Officer
Northwell Health
New Hyde Park, NY

an interview by Daniel R. Roach

This interview with **Greg Radinsky** (gradinsk@northwell.edu) was conducted in October 2018 by **Daniel R. Roach** (daniel.roach@optum360.com), Chief Compliance Officer for Optum360, LLC in Eden Prairie, MN.

DR: Healthcare compliance was not a typical career path 20 years ago. How did you get started?

GR: I was always interested in healthcare because my father was a physician. Hearing my dad's insights into the challenges that were faced by healthcare professionals made me realize that I could make a difference by following my own path. I also had an interest in the law, so I decided to combine these two interests. I grew up in St. Louis, Missouri, and St. Louis University had the top-ranked health law program. I decided to attend St. Louis University School of Law, where I honed in on healthcare compliance. I published an article on the Stark Law and also one of the first articles on how a healthcare organization can manage risk by creating an effective compliance program. This was at a time before there was any published OIG compliance program guidance or corporate integrity agreements.

DR: How did you land a job at the OIG after law school?

GR: I guess you could say it was some luck and some persistence. I had a job offer to work at a law firm in St. Louis, but I thought being in Washington, DC, where federal healthcare laws get vetted and signed, would provide me an invaluable experience to learn health law. So, on my own dime, I flew out to Washington, DC to interview with some law firms. Through contacting an alumnus of my law school, I learned the OIG was interviewing for some new entry-level attorney positions. While visiting DC, I was fortunate enough to schedule an impromptu interview with the OIG.

DR: You spent years at the OIG prior to moving into Compliance in the private sector. How did your experience at the OIG help you when you moved into a compliance role?

GR: My OIG experience turned out to be very helpful. In Compliance, it is difficult to be effective without building consensus within your organization to implement various compliance initiatives. Even within government agencies, a large amount of consensus and communication is needed to effectively align government interests on resolving a compliance matter. My experience at the OIG allowed me to better understand how to get various stakeholders with different views to agree on a resolution. I also received invaluable knowledge about the government's viewpoint through working on fraud and abuse matters and negotiating corporate integrity agreements, which has allowed me to better spot what the government may view as a compliance issue.

DR: Compliance officers frequently interact with the OIG when an organization's behavior is being scrutinized. Based on your experience, what can compliance professionals do to make those interactions more effective, or what do they most frequently get wrong?

GR: It's all about communication! Some compliance professionals may be hesitant to contact the government to ask a question. They should not be afraid to proactively reach out to the OIG staff. As with any relationship, it is important to have good communication, which will build trust. Often, it is hard to build a strong relationship over the phone or internet. I would encourage compliance professionals to meet OIG staff in person to build a stronger connection.

DR: In retrospect, were there any misconceptions about compliance and human behavior that you realized you had after leaving the OIG and moving into the private sector?

GR: Well, when I was working with the OIG, I figured if you fine an individual or organization that violates a law, they will learn their lesson. However, now that I better understand human behavior in different forums, I realize that financial or employment-related sanctions only motivate certain individuals so much. In the private sector, other approaches to compliance are important in building a culture of compliance. It is important to understand that some individuals are motivated by non-punitive measures such as incentives. The more we can understand human behavior, the better we will be at motivating employees to complete their work in an ethical manner.

DR: Why did you leave government practice?

GR: In addition to the law, I have always had an interest in the business and policy side of healthcare. After serving as a fraud-and-abuse attorney at the OIG, I went back to being a full-time student. I obtained my MBA at the Kellogg School of Management. It was a great experience and has allowed me to be both a better attorney and a better compliance professional.

DR: Tell me about your job in marketing and how it affected your compliance career.

GR: After graduating from business school, I tried to

leverage my business experience and took a job in marketing for a large medical device manufacturer. I evaluated business ideas, created business plans, and helped market medical devices to physicians. It was eye-opening to be on the complete opposite side of my role at the OIG, where I investigated medical device manufacturers' marketing practices. It was one of the best things I ever did. It allowed me to see firsthand the business challenges companies face when complying with certain regulations and figuring out solutions that were workable under the law.

DR: Was it hard to switch from an enforcement role to a business function?

GR: At the time, the AdvaMed Code, the industry code of ethics for the medical device industry, had just been released, so there was a lot of attention around medical device companies' interactions with physicians. I do recall some of the physicians I interacted with being a bit perplexed and saying, "You worked for the OIG and you now do marketing?" I was fortunate to work for a medical device manufacturer that was receptive to employees with transferable work skills, and they valued my government experience. I also had legal and consulting roles with that company.

I do recall some of the physicians I interacted with being a bit perplexed and saying, "You worked for the OIG and you now do marketing?"

DR: You have served in both legal and compliance roles throughout your career. What is the key difference in the role of the lawyer and the role of the compliance officer?

GR: A primary difference is that a lawyer's job is to defend the organization, whereas compliance officers are often tasked with helping prevent and detect potential compliance issues by running its compliance program. The in-house counsel and compliance professional roles are constantly evolving, and some functions overlap. The key is that both Legal and Compliance departments communicate their related work to each other.

DR: Please tell me about your current job and how long you have been there.

GR: I serve as the Chief Corporate Compliance Officer for Northwell Health, the largest health system

and private employer in New York. When I started this job 11 years ago, the organization was about half its size, and I had a staff of 14 people. Today, my organization has more than 67,000 employees, and I oversee the compliance function with a staff of approximately 70 employees.

DR: How is your role as the compliance officer different than what you expected when you first took the role?

GR: HIPAA has always been important, but there was less industry enforcement around it 11 years ago. I did not envision spending as much time on data privacy and security issues. Most of the bigger compliance matters involved coding and billing issues when I started. The speed of resolving issues is more important today as well. There are now more defined regulatory time frames to report certain issues, and a compliance issue can go viral instantly with social media.

DR: Did business school help you with your compliance role?

GR: During business school, I learned about developing business plans and marketing products and services. It allowed me to think of a compliance program as a product to market. At Northwell Health, I worked on the branding of our compliance program and a communication strategy to get the word out about it. I also took a more novel approach to creating Northwell Health's annual compliance risk assessment. It included many items that would be part of a regular business plan—financials, business metrics, etc. The idea was for the risk assessment to be viewed not only as a compliance document, but as a valuable business document as well.

DR: In your experience, what is the biggest obstacle to building an effective compliance and ethics program?

GR: Sustaining support at all levels of the organization—not just at the top. When I was in government, I handled many different types of cases against all types of healthcare providers and suppliers. I found that even a single individual can be a big obstacle in not fostering an environment where a compliance program can flourish. The government today is focused even more on individual accountability. There should be zero tolerance for those who do not support a compliance program. If not addressed, it can lead to others thinking it is okay to behave that same way and weaken the organization's compliance culture.

DR: Is the culture of the compliance profession different than the culture of the legal profession? If so, how?

GR: Every organization and department may have its own distinct culture. Notwithstanding, the compliance profession, in contrast to the legal profession, is composed of more staff with different career backgrounds, given the functionality of a Compliance department. My current Compliance department has staff with backgrounds in legal, business operations, marketing, government, clinical, coding, auditing, IT, and research. This diversity allows compliance professionals to interact and learn from various perspectives in trying to solve an issue.

DR: Compliance and ethics programs are fundamentally about shaping human behavior. In your experience, what causes people to behave inappropriately, and what tactics have you used to help employees and leaders make good decisions?

GR: People are influenced to behave inappropriately when they are given unrealistic business goals, grapple with competing interests, and are fearful of retaliation or not pleasing a superior. To combat this, it is important for both managers and leaders to understand the motives of their staff and create an environment where employees at all levels can openly share their concerns. A strong message about the company's ethical values helps employees and leaders make good decisions. At Northwell Health, we include an ethical decision tree in our code of conduct to help employees with these decisions and encourage reporting without retaliation. We even post information about compliance hotline statistics on our public webpage to support trust in our investigatory process.

DR: From your perspective, what are the most important contributions that senior executives can make to support an effective compliance and ethics program? Board members?

GR: Senior executives need to have the Compliance department's back. It is more than just supporting a compliance program in a company's organizational chart. The Compliance department should have the same respect and importance as any other department. Board members' continued support is important as well. An important contribution

for board members is to ensure that the compliance program has appropriate resources to effectively assure compliance.

DR: What are the key compliance metrics that your senior leaders and board members need to see?

GR: At Northwell Health, we share many compliance metrics and data with our senior leaders and board members. We produce lengthy annual and semi-annual risk assessments, and on a regular basis, we provide summary documents of internal and external audits, helpline calls, and HIPAA breach incidents. We place an emphasis on helpline calls and the resources it takes to close them out. We want to ensure leadership is aware of resources utilized and needed to resolve compliance inquiries.

Don't put the pressure of resolving every problem on yourself. Build internal alliances and compliance friends to support the initiatives you take on.

DR: What other data metrics do you use to demonstrate compliance effectiveness?

GR: Compliance is no longer only about having the basic required elements of a compliance program. At Northwell Health, we try to take advantage of the publicly available data tools to design ways to demonstrate compliance effectiveness. For example, compliance professionals can use PEPPER [Program for Evaluating Payment Patterns Electronic Report] data, CMS Open Payments data, and CMS utilization and payment data to provide their compliance program with a checkpoint in those areas. We also use a data mining software product and privacy and security monitoring tools to help identify potential risk areas. The advancement of technology will continue to increase the sophistication of a Compliance department's work and allow compliance programs to better measure their efforts.

DR: There are many students considering a career in compliance. What are the best things about a career in compliance, and would you do it again?

GR: The best thing is never being bored! I would do it again without hesitation. Every day I am exposed to something different. I never expected to be in the same function for so many years, but there was no reason to change. The business, regulations, and delivery of healthcare are complex, and compliance professionals can play a meaningful role in helping organizations deliver healthcare services and products. Today, I would tell students that there are even more opportunities in this field, and it continues to garner respect in the business arena.

DR: What key skills should new compliance professionals hone to help them be more effective?

GR: Be well rounded! Compliance professionals can show their value by having expertise in more than one area. Don't be afraid to learn something new. Compliance professionals should try to get certifications in new areas and learn about other healthcare sectors to help advance their careers. This will be helpful as healthcare consolidation occurs at a faster rate. People skills are also critical. That can be a huge differentiator. It is hard to tell people they can't do something (a frequent response of compliance professionals). If newcomers can teach employees to find compliant solutions, it will be sure to make them more effective instead of just saying "no."

DR: Do you have any parting words of advice for compliance professionals?

GR: There can be stress in working in any job, but the compliance field is noted for having more. Don't put the pressure of resolving every problem on yourself. Build internal alliances and compliance friends to support the initiatives you take on. I was fortunate enough to have fantastic bosses and mentors along the way, and I also have had a great staff to support me. Be creative in finding resources to support you, and don't do it alone.

DR: Thank you, Greg, for sharing your experiences with us. CT

Using enforcement examples

by Catherine Boerner

Sometimes it is hard to keep compliance committee members engaged in compliance program training, compliance risk areas, and compliance program activities. You might want to consider providing and discussing recent enforcement examples from several different sources once in a while. These examples can be used to have a discussion on "Could this happen here?" It might allow committee members to acknowledge what controls are in place to prevent or mitigate the risks that these compliance violations present.

On the OIG website, under "Fraud," go to the "Enforcement Actions" section (*http://bit.ly/2QhlkDx*) to pull some of the examples from the following categories:

Criminal and Civil Enforcement

October 15, 2018; U.S. Attorney; Northern District of Iowa
Iowa Nurse Who Took Pain Medications from Nursing Home Patients Pleads Guilty

An Iowa licensed professional nurse (LPN) who took pain medications from the residents of two nursing homes in 2016 and 2018 pled guilty today in federal court in Cedar Rapids.

September 28, 2018; U.S. Department of Justice
Kalispell Regional Healthcare System to Pay $24 Million to Settle False Claims Act Allegations

Kalispell Regional Healthcare System (KRH), along with six subsidiaries and related entities, have agreed to pay $24 million to resolve allegations that they violated the False Claims Act by paying physicians more than fair market value, and by conspiring to enter into arrangements that improperly induced referrals.

State Enforcement Actions

October 4, 2018; U.S. Attorney; Western District of Pennsylvania
Greensburg Doctor Charged with Illegally Distributing Controlled Substances and Health Care Fraud

A family practice physician has been indicted by a federal grand jury in Pittsburgh on charges of unlawfully dispensing controlled substances and health care fraud, United States Attorney Scott W. Brady announced today.

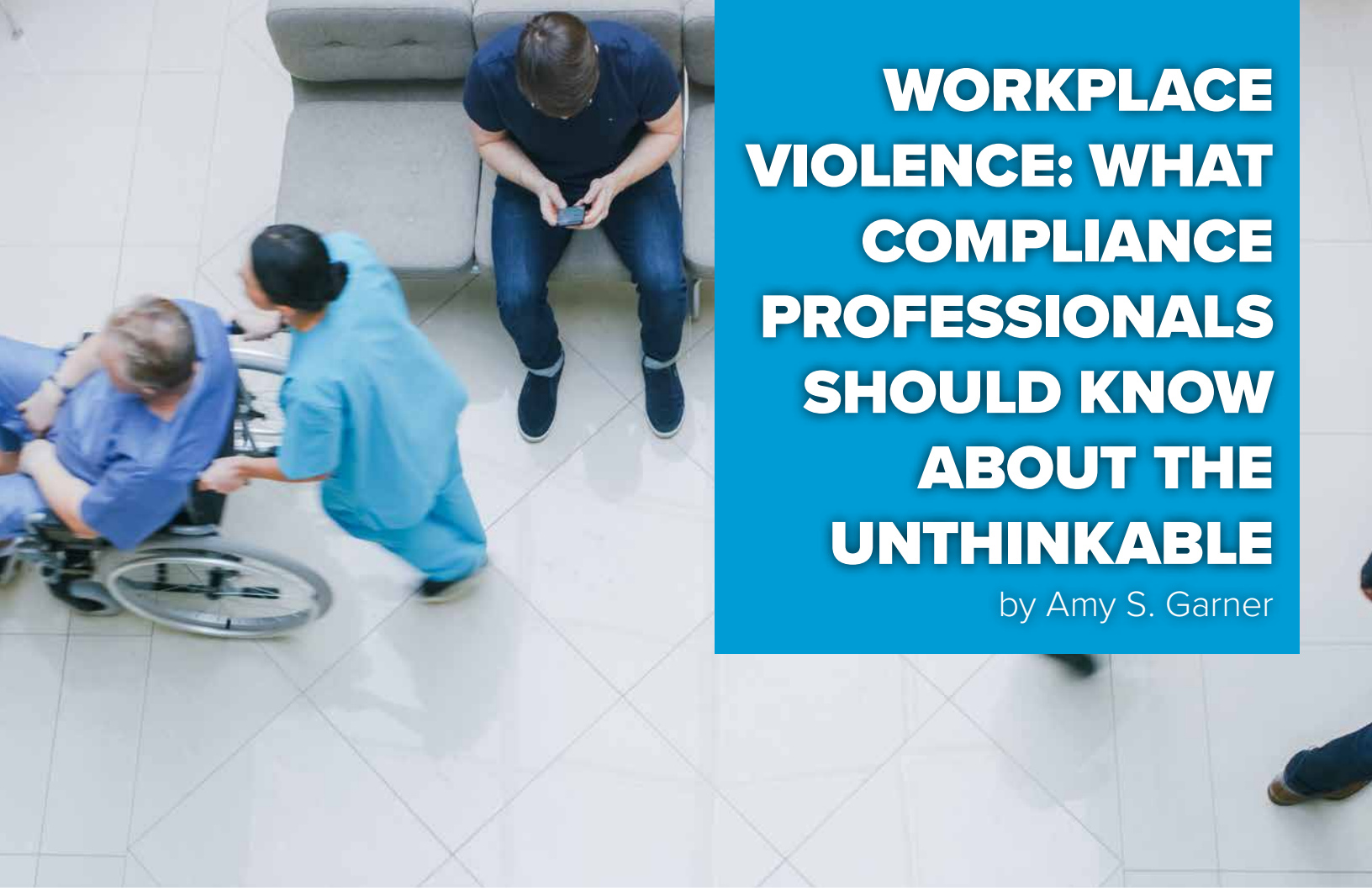
Civil Monetary Penalties and Affirmative Exclusions

09-27-2018
New Jersey Health Center Settles Case Involving Excluded Individual
Newark Community Health Centers, Inc. (NCHC), New Jersey, entered into a $98,750.36 settlement agreement with OIG. The settlement agreement resolves allegations that NCHC employed an individual who was excluded from participating in any federal health care program. OIG's investigation revealed that the excluded individual, a physician working in quality assurance and risk management, provided items and services to NCHC that were billed to federal health care programs.

It can be helpful also to monthly or quarterly provide a compliance awareness email to senior leaders with a list of these enforcement initiatives with the links to read additional details. CT

Editor's note: You may also select headlines published in Compliance Weekly News (*hcca-info.org/cwn*).

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



WORKPLACE VIOLENCE: WHAT COMPLIANCE PROFESSIONALS SHOULD KNOW ABOUT THE UNTHINKABLE

by Amy S. Garner

Amy S. Garner
MBA, EJD, CHC
(amy.garner@wth.org) is Chief Compliance and Communications Officer at West Tennessee Healthcare in Jackson, TN.
@amygriffin96

According to the Occupational Safety and Health Administration (OSHA), approximately 75% of nearly 25,000 workplace assaults reported annually occurred in healthcare and social service settings.[1] Workers in healthcare are four times more likely to be victimized than workers in private industry.[2] Although these numbers are staggering, even more frightening is the fact that most incidents of verbal or physical abuse are not reported by healthcare workers.

Healthcare organizations across the county are making the prevention of workplace violence incidents a top priority. Numerous resources are available to aid organizations in their proactive efforts to train staff, make sure policies and procedures are in place, and assess environmental security. For example, the American Society for Health Care Risk Management has published a workplace violence toolkit to aid in assessing the proactive steps to take to prevent patient-to-staff violence as well as visitor/family-to-staff violence and even staff-to-staff violence.[3]

The Joint Commission also published a Sentinel Event Alert in April 2018 dedicated to physical and verbal violence against health care workers.[4] There are numerous resources available from OSHA, the Centers for Disease Control and Prevention (CDC), and the Crisis Prevention Institute.

It is important to be proactive and train staff on the steps of de-escalation, self-defense, and on what to do when someone is wielding a deadly weapon, but what do hospitals do when the unthinkable happens? What do you, as a compliance or privacy officer, need to be prepared for after the initial incident is over? Chances are the compliance and privacy officer will be involved in both internal and external investigations. This article describes a few of the regulatory

agency considerations that hospital compliance and privacy officers should be aware of in the course of investigating or managing the activities immediately following incidents of workplace violence.

Conditions of Participation for Hospitals

Hospitals are required to meet certain safety requirements to be eligible to participate in Medicare and Medicaid programs. The following areas should be included in training to prepare for incidents.

Emergency Department violence

In some incidents of workplace violence, patients who are in hospital Emergency Departments (ED), due to mental illness or substance abuse issues, may be the perpetrators of the violence. Hospitals that provide emergency services are required to comply with the Emergency Medical Treatment & Labor Act (EMTALA).[5] They are required to provide a medical screening examination (MSE) by a qualified medical professional (QMP). An MSE includes all tests and treatments necessary to stabilize an emergency medical condition. When an incident of violence takes place in an ED, surveyors may investigate to determine if the patient (and perpetrator of the violent attack) received the proper stabilizing care. It is important to review all medical record documentation to determine if EMTALA policies and procedures have been followed and if the patient was treated appropriately.

Because staff members may judge themselves harshly and with great emotion after an event has occurred, it might be valuable to engage an objective clinician to review documentation and be prepared to speak with investigators. Unfortunately for hospitals, surveyors have the advantage of hindsight in these types of situations in that they know the final outcome was an incident of violence. Because of this hindsight, it is important to have someone review medical records without letting the knowledge of the outcome cloud the reviewer's judgment.

Patient rights: Restraints

In certain situations, when a patient becomes violent, it may be necessary to restrain the individual. According to the Conditions of Participation (CoPs) for hospitals, all patients have the right to be free from restraint or seclusion, in any form, imposed as a means of coercion, discipline, convenience, or retaliation by staff. Restraint or seclusion may only be imposed to ensure the immediate physical safety of the patient, a staff member, or others.[6] Additionally, the interpretive guidelines found in the CMS *State Operations Manual*, Appendix A, state that "if a weapon is used by security or law enforcement personnel on a person in a hospital (patient, staff, or visitor) to protect people or hospital property from harm, we would expect the situation to be handled as a criminal activity and the perpetrator be placed in the custody of local law enforcement."[7] It is important to train staff on the role of external law enforcement officers and internal security staff and in the safe application of restraints.

Policies and procedures need to be clearly defined regarding the use of handcuffs, tasers, or other devices, which are prohibited from use on patients other than by law enforcement. Contracted law enforcement officers may be considered to be contracted hospital security personnel, and may only be allowed to act as internal security personnel in compliance with hospital policies and procedures, so it is important to distinguish between the two types of personnel.

It is important to review all medical record documentation to determine if EMTALA policies and procedures have been followed and if the patient was treated appropriately.

Patient rights: Right to privacy

Under the CoPs, patients have the right to personal privacy.[8] When a violent incident occurs, hospitals face a number of issues with regard to patient privacy. There may be media outlets, law enforcement investigators, healthcare oversight agencies, and others that request information about the patient who was the perpetrator of the attack and the victims. The victims of such an attack may also be patients if the facility has to provide medical treatment due to the injuries.

In addition to the CoPs, both federal and state laws require hospitals to maintain confidentiality of protected health information; however, there are exemptions for law enforcement investigations and investigations conducted by agencies tasked with healthcare oversight. Staff members should be trained on all policies and procedures regarding compliance

with privacy standards, and the privacy officer should be involved in assisting with investigations to determine if information can be disclosed without authorization of the patient. Media relations personnel and public information officers should be trained on privacy policies, and they should be the primary contact for requests for information by the media.

Social media and photography

Facilities should have policies and procedures in place regarding the use of social media and the use of cell phones and photography, and staff should be trained on these policies. Unfortunately, almost everyone has a cell phone handy and uses them to take photographs and post photos and videos in real time. In situations where there is a tragic event, the risk to hospitals is that bystanders and employees may photograph or video and post items to social media accounts. Hospitals should be prepared to respond when this occurs, or there may be penalties under federal or state privacy laws.

OSHA requirements

There may be additional reporting requirements to OSHA or the state-equivalent agency when injuries occur in the workplace. There should be a clear point of contact who reports incidents of workplace violence to the appropriate agency within the required time frame. For example, some agencies have limited time to report incidents. A state agency may require that work-related fatalities must be reported within eight hours. All incident-related hospitalizations, amputations, and a loss of an eye must be reported within 24 hours of finding out about the incident in some states.

Accreditation standards

Hospitals may be accredited by agencies, such as The Joint Commission, and may be required to report incidents to the accrediting agency within a limited time frame. Accreditation contacts should be prepared for an investigation by the accrediting agency as well as state survey agencies. In a recent Sentinel Event Alert published by The Joint Commission, all standards related to the issue of workplace violence are listed. Additional Joint Commission resources on this topic are available for facilities that are accredited.

Conclusion

Even though hospitals are prioritizing efforts to prevent incidents of workplace violence against healthcare workers, it is also important to prepare for the aftermath if a tragic event happens. Compliance and privacy officers may believe that it is unthinkable that an intersection exists between the compliance program and incidents of violence, but statistics show that the number of incidents is on the rise. Proactive compliance and privacy officers should prepare for investigations and regulatory agency surveys after such an event occurs. Hospitals should include compliance and privacy officers in their emergency preparedness training events and in post-incident investigations. Hospitals should assign primary contacts for each regulatory agency that requires information related to the incident. It may be unthinkable for these types of events to occur in our hospitals; however, it is time for compliance and privacy officers to think about their roles during the aftermath. CT

Endnotes

1. Occupational Safety and Health Administration, *Guidelines for Preventing Workplace Violence for healthcare and social service workers*, 2015, 3148-04. https://bit.ly/1al3BSr
2. Security Industry Association and International Association of Healthcare Security and Safety Foundation, *Mitigating the Risk of Workplace Violence in Health Care Settings,* August 2017. https://bit.ly/2yWeERp
3. American Society for Healthcare Risk Management, Workplace Violence Toolkit. https://bit.ly/2F0ksyr
4. The Joint Commission, Sentinel Event Alert 59: Physical and verbal violence against health care workers, April 17, 2018. https://bit.ly/2Kf4eA6
5. 42 CFR 489.24 (Special responsibilities of Medicare hospitals in emergency cases). https://bit.ly/2yQXynL
6. 42 CFR 482.13(e) (Standard: Restraint and seclusion). https://bit.ly/2yWeZUb
7. Centers for Medicare and Medicaid Services, *State Operations Manual, Appendix A – Survey Protocol, Regulations and Interpretive Guidelines for Hospitals,* Section 482.13(e), 2015. https://go.cms.gov/1Ryqelk
8. 42 CFR 482.13(c) (Standard: Privacy and Safety). https://bit.ly/2yWeZUb.

- Healthcare workers are four times more likely to be involved in a workplace violence incident than workers in other industries.
- Compliance and privacy officers may not realize the importance of being prepared for incidents of workplace violence.
- Compliance and privacy officers should prepare for both internal and external investigations immediately following incidents of violence.
- Hospitals in particular are required to comply with various regulations and standards that may be implicated when a tragic incident occurs.
- Hospitals should assign primary contacts for each regulatory agency that requires information related to an incident of workplace violence.

Happy New Year!

by Lynda Hilliard

The New Year brings a sense of new beginnings. We make personal, work, and career resolutions and, for as long as we can sustain it, initiate changes that will make positive impacts on our lives. Let's bring this sense of renewal to our workplace and resolve to accomplish our goals and objectives in an efficient and effective manner. We should also involve our employees and our interactions with them by providing a foundation for them to improve and change as well.

For a majority of organizations, January is the beginning of the fiscal year, and new budgets and operation plans become effective. For this column, let's assume we are all on this calendar format. For the most part, our workloads have been imagined and budgeted months before; and now is the time to review those budgets, determine our plan for the next 12 months, and ascertain whether they still meet the needs of the department. We review work volume, productivity, staffing, and education resources estimates—myriad elements of the budget as they relate to the Compliance department's annual work plan, especially the audit plan. Has anything happened, either at our organization or in the industry, that has instigated a reevaluation of the risk assessment and adjusted the prioritization of organizational risks? Depending upon the results, we need to reassess our budgeted resources to adjust for additional investigations, audits, or education and training.

Why should we alter our plans for this year? Why can't we just follow our budget and approved annual work plan? Budgets and work plans are great tools to focus our use of limited resources and participation in a larger effort to meet organization and department-wide objectives. However, in healthcare compliance, we are tasked with continually surveying our community, regional, and national industry environs to detect potential compliance risks, and then initiating efforts to deter or mitigate that risk. It is an ongoing effort that results in a more effective compliance program—one that continues to evolve over time. New patient programs or revenue enhancements can combine with new or revised financial or patient charging systems to form potentially new compliance risks that should be reviewed and mitigated.

It is a new year, and a new opportunity to make a difference. Learning to continually scan the environment for potential regulatory risks will enhance efforts to detect, deter, and prevent instances of fraud, waste, and abuse. CT

Lynda Hilliard

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

CONTROLLING MOBILE DEVICES IN AN ACADEMIC MEDICAL CENTER: UNIQUE CHALLENGES

by Marti Arvin

Marti Arvin

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

bit.ly/in-MartiArvin

In today's healthcare environment, mobile devices are rampant. Controlling the nature and method of data stored on these devices is not easy in most industries—and mobile devices in the healthcare environment present a unique challenge. What makes securing mobile devices particularly difficult in healthcare and even more difficult in the academic medical center (AMC)? It helps first to understand the environment.

The academic medical center

The old saying is that, "If you have seen one AMC, you have seen one AMC." The organizational structures, politics, and cultures vary among AMCs. The nature and structure of the legal entities involved can also vary, but there are consistent factors. Usually, there is a healthcare facility, such as a hospital, and an AMC will have faculty members and trainees (i.e., residents and students). The clinical activity of the faculty members will often be performed through one or more faculty practice groups. Clinical research is often also being conducted simultaneously on the university side. Regardless of the structure, controlling the data on mobile devices is difficult, but sometimes the AMC structure can make an already complex proposition even worse.

So, what are some of the variations of the structures? There can be a single legal entity in which the university owns the hospital and faculty members are employed by the university, both as educators and clinicians. All research activity is performed by that legal entity, and most of the training programs are all conducted by the entity.

Another variation is that the university is one legal entity responsible for most of the training programs and research activity, and the health system is another legal

entity or a combination of related legal entities. Yet another variation is a combination of the first two (i.e., one or more of the hospitals are a component of the university and the health system owns others) where all entities share common governance and oversight.

There may also be one or multiple affiliated hospitals that are each an independent legal entity with a separate governance structure. One or more faculty practice groups generally employ the physicians. The faculty practice groups may be affiliated but separate from the university. A practice group may be a component of a large health system or completely independent from it. When the practice group is a separate legal entity from the university, the faculty members are generally dual-employed. They are university faculty performing educational and research activities for the university while, as clinicians, they are performing patient care services through the faculty practice group.

Mobile devices in these environments

What are the implications for mobile devices? Most physicians do not want to have two of everything (e.g., phones, computers) for their clinical work and faculty/research work. Many universities and some health systems don't want to buy computers for everyone. If the university or the health system supplies the devices, the brand of the device and the features on it are often not the most high-end. If the organization supports Apple devices but the end user prefers Android, it usually results in a bring-your-own-device (BYOD) structure. And if the university or health system does not provide the device at all, it leaves only a BYOD structure.

Securing devices the AMC doesn't own

The perfect solution doesn't exist, but there are ways to control what data can be stored on certain devices. The first step is to start with a policy. This simple solution is likely the least effective, but it will establish the foundation for all other controls. An organization can have a policy stating that no sensitive data, such as protected health information (PHI), personally identifiable information (PII), or proprietary information, can be stored on a mobile device unless it is encrypted. Enforcement of such a policy would be next to impossible without other controls.

The organization can use a technology solution to help ensure data is protected. The solutions will vary depending on the device and method of protection. Many technology solutions will support different types of devices. For example, the organization may set up the network and servers so that only registered laptops can be connected. These controls, typically certificate-based, will allow the device to be remotely managed and can ensure a password standard, patch level, and encryption are enabled. It is also important to have a remote-wipe capability if the device is lost or stolen. These controls should be defined by the organization and be leveraged as the minimum threshold to permit connections.

Portable external drives present a significant risk because of the high probability and impact of loss. Again, technical solutions can encrypt all data saved to such a removable drive. This effectively mandates the encryption "safe harbor" solution to prevent a data breach; however, it may not be a solution in every instance. If a mobile phone is connected as an external storage device, the technology solutions may not encrypt the data going to the phone. Additionally, these solutions may not secure files created on the external drive. Other technology solutions can evaluate the external drive when it is plugged in to the computer to ensure the device is encrypted. Some organizations have taken the step of disabling the USB drives on computers before they are deployed to the workforce and only allow the drives to be enabled on an exception basis. This would only work if the organization supplied the computers to its workforce but, in a BYOD world, that solution would not work.

The perfect solution doesn't exist, but there are ways to control what data can be stored on certain devices.

In a BYOD environment, these solutions come with more baggage. These same issues occur if the organization considers providing encryption software to end users for their personally owned devices. For example, does the organization's license for the software permit it to be loaded on a device not owned by the organization? What happens if the individual's computer is somehow damaged or corrupted

by the process of installing the software? What if the user has not kept up to date on system patches? What if the individual's computer is incompatible with the version of the encryption software the organization is using? What if the health system wants to provide encryption software, but the device is owned by the university? What if the end user objects to the technology solution for privacy reasons?

The organization may also choose to provide encrypted external drives for users. But what happens to those drives once the user, such a resident or student, is no longer with the organization? What happens to the organization's data that is on any of the devices discussed thus far? Organizations need a process for getting their own devices back and ensuring only data that is approved can go with the user when the user leaves the organization.

Organizations may consider requiring an attestation from any user who had access to sensitive information when that user leaves the organization. In that attestation, it can state that either the user has no sensitive information or that any sensitive information they are taking has been approved by the appropriate authority and is now their personal responsibility. If the user refuses to sign the attestation, the organization can document this and inform the user that any sensitive data that is removed from the organization will be considered a theft.

Most of these are issues that any hospital, physician group, or other provider may need to deal with regarding the security of mobile devices, but what makes it more difficult in an AMC? First, as previously discussed, there can be multiple legal entities that

have various concerns. Each entity may have different risk tolerances, different budgets to support the end user, and various controls to help protect data. When there are multiple organizations, the effort to secure mobile devices needs to be coordinated and easy to follow by the end user. If the hospital has one policy, the university might have a slightly different policy, and the physician practice group could have yet another policy. With multiple policies to follow, the user who works in all three entities will find it difficult to be compliant with all of them. As a result, the risk increases that the user will follow whatever policy they find easiest, which is typically the least restrictive policy or something they make up.

Academic freedom

Another unique challenge in an AMC is the concept of academic freedom, which is the premise that says faculty and students should be free to engage in intellectual debate without fear of censorship or retaliation.[1] The concept allows faculty and students the right to express views in an open manner. However, this concept is often invoked by faculty when they are concerned that policies and controls that the university or AMC wants to implement will constrain them, even if it is not something that limits their ability to engage in a free and open intellectual discussion. Academic freedom does not permit a faculty member to "ignore college or university regulations," but it certainly allows them a way to express their disagreement with such regulations.[2]

Academic freedom may be something that faculty members attempt to invoke if they are unhappy with an organization's

implementation of any of the solutions discussed above. So, making sure everyone understands what the policy and solutions are designed to protect and not protect is important for an organization trying to ensure good data protection practices. Such good practices should not be implemented in a manner that would impinge on academic freedom.

The Family Educational Rights and Privacy Act

Another area of concern for AMCs is the data of students under the Family Educational Rights and Privacy Act (FERPA). The way this data is maintained can also create risks. If employees and faculty are keeping this type of data on mobile devices, there could be issues for the organization if the data is not properly secured.

Although there is no specific regulatory obligation to notify students of a breach of their data, similar to that under HIPAA, the Federal Department of Education (DOE) has taken the position that universities who receive Title IV federal student aid (FSA) funding must notify students of a breach or suspected breach of any data, not just FSA data. The authority for this position has yet to be played out. DOE has stated this is a requirement under the Student Aid Internet Gateway (SAIG) Agreement signed by the institution.[3] This is certainly another area for AMCs to keep their eyes on. DOE has threatened fines for non-compliance and indicated it could withdraw Title IV funding if the college or university cannot demonstrate a robust security program.[4]

Conclusion

The challenges and cost of trying to protect sensitive data will only continue to increase in AMCs, so an AMC must assess its risk tolerance. The risk to PHI carries regulatory sanctions if it is not properly protected. The risk of not properly protecting other types of sensitive data that may not be PHI may also carry regulatory risks. For example, individually identifiable information is not always considered PHI. It depends on how it was collected and the organizational structure of the entity holding it. If it is PHI, it too is protected by HIPAA. If the sensitive, individually identifiable data maintained about research subjects is not PHI, there may still be state laws protecting it. The same may be true for individually identifiable information maintained about employees.

All healthcare entities have challenges when ensuring sensitive data on mobile devices is secure. However, the unique and varied structure of an AMC creates additional challenges in that environment. Not only must they contend with HIPAA regulations, but they also must consider FERPA data. They must also ensure that any solutions used to help secure information meet the technical demands of the environment as well as ensuring that the solution does not infringe on concepts such as academic freedom. This is a daunting, but not impossible, task. It takes coordination among the business units if the AMC is a single legal entity and among the different legal entities if there is more than one.

The obligations to protect sensitive information are likely to increase rather than decrease over time. Being prepared to meet those challenges through a strong information privacy and security program continues to be one of the best defenses. CT

Endnotes

1. Cawry Nelson, "Defining Academic Freedom," *Inside Higher Ed*, December 21, 2010. https://bit.ly/2cG1ak9
2. Ibid.
3. U.S. Department of Education, Federal Student Aid Office: Frequently Asked Questions about Cybersecurity Compliance. https://bit.ly/2EXsOXF
4. Ibid.

- Information security and privacy challenges are present in all healthcare organizations.
- Academic medical centers (AMCs) may have additional challenges not present in other healthcare organizations.
- Understanding what academic freedom is, versus what it is not, is key.
- There are regulatory enforcement agencies beyond OCR to consider.
- Coordinating efforts between multiple parties will increase the success of the AMC's information privacy and security program.

Resolution empathy: Achieve better patient outcomes

by Sharon Parsley

During late 2018, I experienced a good portion of our healthcare delivery system from a bedside seat, in the role of advocate and spouse. Injuries sustained by my husband resulted in a first-ever ambulance ride to a Level 2 trauma facility, four days as a guest of a medical intensive care unit, two days in a trauma step-down unit, 12 days in an inpatient rehab facility, and a discharge home with nursing and physical and occupational therapy services. On a daily basis, we experienced uplifting, thoughtful, and empathetic interactions with the vast majority of his caregivers. On the flip side of the coin, there were conversations at key decision-making points that were handled hurriedly and ineptly by clinicians, with little compassion or care in evidence.

This experience caused me to consider and research what, if any, correlation exists between patient outcomes and patient-clinician relationships. I am not a statistician (nor do I play one on television), so I relied on open source published works by others, and here simply summarize (in non-technical terms) the key conclusions from two journal articles I found interesting.

The first article, published in the *British Journal of General Practice*, opens with the statement that "Patients consider empathy as a basic component of all therapeutic relationships and a key factor in their definitions of the quality of care."[1] While ultimately opining that further research is needed, this article concludes that empathy demonstrated by a patient's physician yields improved patient satisfaction and compliance, and reduced patient anxiety and distress.

A *PLOS ONE* article synthesized results from 13 randomized clinical trials evaluating one or more objective (e.g., blood pressure) or validated subjective (e.g., study participant pain scoring) outcomes.[2] Findings here were that the patient-clinician relationship has a "small… but statistically significant…effect on healthcare outcomes." While categorized as "small," the quantified relationship impact exceeded the effect of aspirin administration on myocardial infarction over five years and also the impact of smoking on male mortality over eight years.

For 2019, let's resolve to demonstrate and reward empathy. Your patients deserve it. CT

Editor's note: In 2019, "The Compliance-Quality Connection" *will be published six times annually: January, March, May, July, September, and November.*

Sharon Parsley
JD, MBA, CHC, CHRC
(sharonparsley@outlook.com) is President & Managing Director of Quest Advisory Group, LLC in Ocala, FL.

Endnotes

1. Frans Derkson, Josien Bensing, and Antoine Lagro-Janssen, "Effectiveness of empathy in general practice: a systematic review" *British Journal of General Practice*. January 2013, e76-84. http://bit.ly/2FJpTSN
2. Kelley J, Kraft-Todd G, Shapira L, et al. "The Influence of the Patient-Clinician Relationship on Healthcare Outcomes: A Systematic Review and Meta-Analysis of Randomized Controlled Trials" *PLOS ONE*, April 2014; Vol. 9, Issue 4, e94207. http://bit.ly/2BBMixy7

COMPLIANCE TIPS FOR IMPLEMENTING AN ELECTRONIC MEDICAL RECORD SYSTEM

by Lisa I. Wojeck

Lisa I. Wojeck
MS, JD, CFE, CISA, CHC
(lisawojeck@gmail.com) is a healthcare compliance professional living in Baltimore, MD.

The electronic medical record (EMR) system is crucial to hospitals, physicians, and other healthcare providers, and arguably the most important system in the provision of care. It also presents some of the greatest opportunity for risk as it relates to federal regulations, and therefore it must be built to comply. Breaches of protected health information (PHI) range from $100 to $50,000 per medical record with a cap of $1.5 million per calendar year.[1] Erroneous claims are false claims, and Medicare does not pay false claims. Further, false claims may result in treble damages, fines, exclusions, and imprisonment.[2] This article provides compliance tips for implementing an EMR system.

There are various phases in the life cycle of an electronic medical record system, including planning, building, testing, deploying, and maintaining it. Compliance should be consulted, if not included in each phase. The project lead responsible for the software may have an information systems and/or a clinical background and may not be aware of compliance issues. It is more helpful to the organization to include Compliance from the beginning, rather than when a problem is identified. Cleaning up errors is more difficult and costly than building the system correctly.

Medicare requirements

There are a number of Medicare manuals and requirements; these are based on federal regulations and must be followed. As information systems teams build the EMR system, they usually meet with the business area. Diagrams, flowcharts, and narratives are created to document a meeting of the minds as to the way the business process works. If the individuals involved in that process do not understand Medicare requirements,

and Compliance is not included, the system may not be compliant with Medicare.

For example, the EMR system build needs a mechanism or mechanisms and workflow to identify surgeries that require device replacements because of defects, recalls, mechanical complication, etc. The purpose of these build features is to enable the organization to generate correct claims and avoid inappropriately charging Medicare for replacement devices due to defects, recalls, mechanical complication, and such.[3]

Outpatient rehabilitation services provide another interesting example. Medicare manuals state that when only one service is provided in a day, providers should not bill for services performed for less than eight minutes. A single timed CPT code in one day is measured in 15-minute increments, and one unit is 8 minutes through 22 minutes.[4] Incorrect builds, including those involving time, will cause incorrect claims, and incorrect claims (whether intentional or not) are false claims. Careful attention must be given to Medicare requirements throughout the lifetime and use of the EMR system.

EMR features

Many systems come with built-in features that should be configured to avoid problems, and all users should be trained how to use these features appropriately.

Copying and pasting

The copy-and-paste feature permitted by EMR systems needs to be vetted by a well-rounded team of leaders at organizations. They need to decide whether they will permit their organization's providers to copy and paste, and if it is permitted, they need to document their policy on the topic. Again, the big concern is the submission of claims that may be false claims.

For those providers that use the copy-and-paste feature, they need to ensure they are removing information specific to the patient record from which they copied the information, and they need to ensure they are incorporating adequate detail in the patient record to which the information is copied. No two patients are identical, and no two patient visits are identical. Further, if care and work is not documented, it is not billable.

Faxing from the EMR system

Faxing from the EMR system is convenient for providers. However, reasonable safeguards need to be established to ensure faxes are sent to the intended recipient to prevent breaches and provide quality care. Without reasonable safeguards, a pediatrician may receive gynecological records they clearly do not need. Also, a provider with a very similar name or the same name as another provider may not receive a copy of the medical record required to provide quality care. For example, it is not acceptable for Dr. Robert A. Jones, pediatric oncologist, to receive records intended for Dr. Robert M. Jones, internist. The internist relies on certain information to make diagnoses and/or monitor conditions. If test results, images, and data are faxed to an unintended recipient, it slows down the communication of this information, or it may not reach the intended provider at all.

The HIPAA Security and Privacy Rules require reasonable safeguards to protect against intentional or unintentional disclosures.[5] These vary from one covered entity to another. In determining reasonable safeguards, each covered entity needs to analyze their own size, business, needs, circumstances, and potential risks to patient privacy. The potential effect on patient care, administrative burdens, and financial burdens should also be considered.[6] The Office for Civil Rights (OCR, the entity that enforces HIPAA Privacy and Security and the Patient Safety Rule) has documented some reasonable safeguards, such as requiring computer security measures including passwords.

In determining reasonable safeguards, each covered entity needs to analyze their own size, business, needs, circumstances, and potential risks to patient privacy.

Applicable reasonable safeguards for faxing start with considering whether faxes need to be sent and whether use of the EMR eliminates unnecessary faxing. The covered entity needs to determine whether the workforce needs to fax intra-organizationally. For those outside the organization, some EMR system technologies have various products available, for example a product that permits non-EMR system users the ability to view certain data elements, and another version that permits users of the EMR system the ability

to view specific data elements of patients from anywhere in the world.

Providers that are outside the organization—and do not use the organization's chosen EMR system—probably need to use fax technology. Reasonable safeguards for faxing must include selecting the correct provider/fax numbers and verifying his/her specialty and address prior to faxing. Use of a fax cover sheet is also very important; the fax cover sheet should, at a minimum, require the sender to complete the TO person, phone number, and fax number; FROM person, phone number, and fax number; and total fax pages. Further, the cover sheet must have appropriate privacy disclaimer language and contact information for a person, potentially the sending organization's privacy officer, that may be contacted if the recipient has questions about why they are receiving the fax. Having hard stops in the process to require reasonable safeguards within the EMR system is ideal.

Notice of Privacy Practices

Patients are required to have adequate notice of how a covered entity may use and disclose their PHI; typically this notice is called the Notice of Privacy Practices (NPP).[7] Although the law does not require patients to sign the acknowledgment of receipt of the NPP, the law requires doctors, hospitals, and other healthcare providers to ask patients to state in writing that they received the notice.[8]

The process of capturing the electronic signature or refusal to sign must be correct. The patient must be provided with the NPP; the patient may be given an opportunity to read the notice on a screen. For those

patients who inquire as to what they are signing, they cannot be misinformed. For example, they cannot be told the signature is for billing purposes. Appropriately building the NPP process into the EMR system sets the organization up for success.

The same applies to other forms requiring electronic signatures. Examples of these form(s) include communication consents and patient belonging releases.

Monitoring access

The Security and Privacy Rule states that the covered entity must, "Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports."[9] This statement implies a proactive review, not a reactive review, and that the review includes all patients, including employees, VIPs, and "ordinary" patients.

Reports generally made available to privacy officers via EMR systems are voluminous transaction logs that contain little if any context and/or perspective. To be effective, testing a sample is required. However, to pull a worthwhile sample, the privacy officer needs to consult with the Human Resources department to add the needed context/perspective (e.g., the user's title, department, shift, and job responsibilities). When the reports are thousands of pages long, this is an exercise in finding enough resources to help look for a needle in a very large haystack.

Consequently, many covered entities have come to the conclusion that EMR companies are very good at EMR systems, and not so good at access monitoring. Software companies do exist for the sole purpose of providing products that

monitor EMR access. Many of these software products use artificial intelligence (AI) to learn user behaviors over a period of time and permit covered entities to write a number of rules, such as "identify users who access patient records belonging to patients that reside on the same street as the user." Based on the system learning every user's behavior and/or the covered entity's rules, the privacy officer is made aware of potential wrongful accesses to investigate. This provides for a manageable starting place to investigate potential wrongful access and activity.

Communicating with patients

Some patients and physicians prefer to communicate with each other by means of email and/or text messaging, which are not secure methods of communication.[10] If the organization makes the business decision to permit these communications, reasonable safeguards must be used. At a minimum, these should include a conversation with the patient informing them:

- that emailing and texting are not secure and may be intercepted;
- about use of the Minimum Necessary standard to limit the release of PHI;
- that their email address and/or phone number will be verified in advance of the communication; and
- that the patient is required to sign an appropriate consent form.[11]

Many EMR systems permit providers and patients to communicate in a secure manner within a portion of the system. Not only does this provide for secure communications, it also permits the information to become a part of the medical record.

If covered entities decide to permit their providers to communicate outside the EMR system, a screenshot needs to be taken of those communications, and the screenshot needs to be scanned into the EMR. If patients voice grievances or file medical malpractice cases, or another type of investigation occurs, these communications will be valuable.

Conclusion

Compliance provides more than audit services; Compliance is a valuable resource and should have a seat at the table when it comes to EMR systems. Failure to include Compliance may result in a poorly developed system that causes covered entities to incur fines and/or penalties and potentially be excluded from federal healthcare programs. CT

Endnotes

1. 45 CFR § 160.404 (Amount of Civil Monetary Penalty)
2. 31 USC §§ 3729 – 3733 (False Claims Act)
3. "Medicare Claims Processing Manual, Chapter 4 - Part B Hospital," CMS.gov, Rev. 3941; December 22, 2017. https://go.cms.gov/1Q5LNeE
4. CMS, *Medicare Claims Processing Manual*, Chapter 5 - Part B Outpatient Rehabilitation and CORF/OPT Services, CMS.gov, Rev. 3995, March 9, 2018. https://go.cms.gov/2PNrLh3
5. 45 CFR § 164 (Security and Privacy)
6. 45 CFR § 164.502(a)(1)(iii) (Incidental Uses and Disclosures). https://bit.ly/2OCtKAm
7. Ibid, Ref #5.
8. HHS.gov, Notice of Privacy Practices. https://bit.ly/2QutHIv
9. 45 CFR § 164.308(a)(1)(ii)(D) (Administrative safeguards, Information system activity review)
10. HHS.gov, "Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?" https://bit.ly/2QutHIv
11. Idem.

- Electronic medical record (EMR) system project leads may not be aware of compliance issues.
- Improperly built EMR systems may cause the covered entity to incur fines and/or penalties.
- Electronic communications outside the EMR system between physicians and patients raise more than privacy issues.
- Although EMR systems may be very good for electronic medical record purposes, they may be limited for other purposes.
- Compliance professionals are valuable resources to covered entities as they make business decisions about their EMR system.

Healthcare Privacy
Basic Compliance Academies

Chicago
March 11–14

Washington DC
June 3–6

Denver
July 22–25

Charleston
August 12–15

Anaheim
September 30–October 3

Las Vegas
November 18–21

Explore the broad spectrum of privacy laws and regulations affecting healthcare organizations during this three-and-a-half-day academy led by trade experts. Topics and discussions go beyond the implementation of compliance programs to explore the latest developments in HIPAA privacy, the Federal Privacy Act, data security, privacy investigations, and more. The Academy is limited to 75 participants to enhance your learning experience. The optional Certified in Healthcare Privacy Compliance (CHPC®) exam is offered on the last day. Separate application and fee required.

Research
Basic Compliance Academies

Chicago
March 11–14

Las Vegas
November 18–21

Increase the effectiveness of your institution's research compliance program during this three-and-a-half-day academy. You'll learn about emerging risks in scientific misconduct, human research protection, grant management, and more—plus, strategies to mitigate risk. Best of all, you'll gain insight from industry experts and have the opportunity to network with other professionals in the industry. The Academy is limited to 75 participants to create a hands-on learning experience. The optional Certified in Healthcare Research Compliance (CHRC)® exam is offered on the last day. Separate application and fee required.

hcca-info.org/academies

HCCA™
Health Care Compliance Association

Getting to 100 percent

by Samantha Kelen

Over the years, I've heard many peers express their frustrations at the effort required to get employees to complete compliance training. It can be one of the most time-consuming activities we undertake. I've even heard folks say, "100% completion rates are just not possible." I may be an optimist, and every organization is different, but I believe 100% is in fact attainable and appropriate as a goal.

In order to reach this achievement, there are a few things you want to consider pre-deployment. First, define what 100% looks like realistically in your organization. Does that include individuals out on leave? What about those retiring during or shortly after your deployment window closes? Are you willing to make exceptions for employees who are unable to complete due to competing critical business needs?

Next, make sure your deployment window and timing are optimal. For example, could you deploy in January and give employees a full year to complete? This could allow employees the flexibility to take the training during a time when their workloads are lighter. However, more time could lead to longer procrastination, which may just prolong the issue. Work with your business unit leaders to pick the best approach.

Once you've gained some clarity on those two points, here are some strategies (both "sticks" and "carrots") to consider employing once your training has been rolled out:

- **Progressive escalations:** One of the more common and benign tools to use is your email. Emailing delinquency reminders, all the way up the chain if needed, is a great way to get an employee's attention.
- **Visible reporting:** My experience has shown that no executive likes to be last. Providing periodic reports to your leadership team could incentivize them to have their group complete the training early on. Similarly, shaming those poor performing business units could give them the kick in the pants they need to make the training a priority.
- **Real incentives:** Everyone likes a prize. Perhaps you could enter the first 100 employees who complete training in a raffle for a gift card. Or you could provide lunch or a few hours of comp time to a department that reaches 100% within an established early deadline.
- **Financial harm:** For those organizations with the appetite, you could impose financial penalties on individuals by docking their pay by a small percentage or to business groups by docking their budget for next year. This will definitely get their attention. CT

Samantha Kelen
MBEC, CCEP
(sam@samanthakelen.com) is a Lead Ethics Analyst at Duke Energy in Charlotte, NC.

TRIED AND TRUE SURVEY READINESS

by Jennifer A. Yang

Jennifer Ann Yang
MPP, CHC, CPHQ
(jennifer.yang@state.mn.us) is the Deputy Chief Compliance Officer at the Minnesota Department of Human Services in St. Paul, MN.
bit.ly/in-JenniferYang

Serving as the compliance officer for a psychiatric hospital, which was under a Systems Improvement Agreement (SIA) with the Centers for Medicare and Medicaid Services (CMS) in the past two years, I had the opportunity to develop and implement a survey readiness framework to assist the facility in preparing for two unannounced, full Medicare certification surveys. With extensive pressure and a tight timeline of approximately six months, the survey readiness team went through a journey of major obstacles and challenges, but nevertheless succeeded.

In this article, I will share the survey readiness framework and provide practical tools and examples. With this framework, the facility successfully completed the SIA requirement of passing both surveys without any condition-level findings. Although this framework focuses on CMS Conditions of Participation (CoPs), other regulatory/accreditation standards can be applied to the framework.

Survey readiness is based on two parts: survey preparation (the year-round efforts prior to survey) and survey performance (the facility's use of resources and response during the survey). Survey preparation depends largely on strong organizational skills and using practical project tools to move teams toward being in compliance and maintaining compliance. Leadership must build a culture that fully accepts and operates on being prepared for a survey 365 days of the year. Staff performance is critical during the week of survey. During this week, the facility must use resources and skills in the most optimal manner. The facility's survey results will depend largely on how effectively and quickly staff respond to surveyors' requests, and how knowledgeable and skilled staff are

in navigating surveyors through patient charts and answering questions and concerns.

Survey preparation

The survey readiness framework has five phases (i.e., assessment, planning, execution, demonstrated competency and validation checks, and taking action) within an ideal timeline of 12 months—a continuous, year-round effort.

Assessment (2 months)

A facility-wide assessment should be conducted based on a comprehensive review of the regulatory standards. It is recommended to conduct a facility-wide assessment at least once every year. Assessments can be based on a comprehensive review of standards, mock surveys, chart reviews, patient observations, or a combination thereof. This effort includes:

- Establishing 12 teams, each team focusing on one or two standards;
- Conducting small workgroup meetings for each team to review the standard(s) and for the facilitator to ask mock survey questions (directly pulled from the CMS Manual) about how the facility complies with the standards;
- Identifying the corresponding policies, procedures, and processes for each standard; and
- Reviewing and analyzing the CMS survey protocols to help identify gaps and opportunities for improvement.

Key tools used in this phase include:

- CMS *State Operations Manual* (Appendix A and Appendix AA), including survey protocols, guidelines, and interview questions.
- CMS worksheets: discharge planning, quality assessment and performance improvement, and infection control.

A critical deliverable for this phase is to develop 12 teams with each team owning a chapter binder—a collection of policies, procedures, and pertinent documents related to the CMS standard(s). For example, a team of six (with the social work director as the lead) is responsible for reviewing, understanding, and ensuring the facility's compliance with the patient's rights standard (42 CFR § 482.13).

Planning (1 month)

Based on the results of the assessment, leadership and the compliance officer strategize survey readiness efforts in preparation for the upcoming surveys. This phase includes:

- Developing a survey readiness plan that reflects both long-term goals and high-priority goals that require immediate action;
- Developing a survey readiness tracking tool to help organize and monitor all identified concerns and corrective actions based on the results of assessment;
- Identifying chapter team leads to establish accountability for compliance-related improvements and corrections; and
- Establishing a survey readiness committee at a leadership level (includes all chapter leads) to ensure oversight of corrective actions and continuous compliance.

Execution (4 months)

The execution phase is initiated with the convening of the survey readiness committee. This committee reviews the survey readiness tracker (SRT) on a regular basis—monthly is recommended. The hospital/facility administrator or a member of leadership is the chair of the survey readiness committee. The compliance/quality staff are directly involved in the committee to help coordinate meetings, facilitate discussions, and to assist the team with achieving project milestones and critical compliance-related deliverables. This committee reviews and discusses action items across all 12 chapters to ensure coordination and collaboration when applicable.

Leadership must build a culture that fully accepts and operates on being prepared for a survey 365 days of the year.

During this phase, the small workgroup meetings continue to take place on a bi-weekly or periodic basis. The role of the compliance officer is to ensure small workgroup meetings are scheduled and work is accomplished within deadlines. The 12 small workgroups will continue to function with a hands-on approach to implement and monitor compliance activities. Each workgroup is responsible for maintaining

Table A: Example Survey Readiness Tracking Tool

NO.	ITEM/ ACTIVITY	CONDITION OF PARTICIPATION CATEGORY	PHASE 1: Documentation Review 2: Training & Education 3: Validation, Audits, & Tracers 4: Corrective Actions	DESCRIPTION NOTE CORRECTIVE ACTION IF PHASE 4	STAFF ASSIGNMENT (a) Lead Staff (b) Quality Staff	PRIORITY 1= BY JAN. 31 2= BY FEB. 28 3= BY MAR. 31 4= LONG-TERM EFFORT"	ACTUAL COMPLETION DATE	STATUS & % COMPLETE TBD: NOT STARTED GREEN: COMPLETED YELLOW: INITIATED & EXPECTED TO MEET DEADLINE RED: PAST DUE
1	Training	Emergency Preparedness	Phase 2 - Training & Education	Develop annual training curriculum and work with educator on implementation and tracking of completed trainings.	(a) Tom (b) Joe	3 = BY MAR. 31	3/25/19	100%
2	Policy	Leadership & Governing Body	Phase 1 - Documentation Review	Review Policy for Contracts and Note any updates needed. Next Phase: train and update policy if applicable	(a) Maria (b) Joe	3 = BY MAR. 31	TBD	50%
3	Discharge Plans	Discharge Planning	Phase 3 - Checks: Conduct Tracers, Audits, and Mock Survey	Check discharge plans for patient signatures and proper follow up.	(a) Dr. Lee (b) Javier	3 = BY MAR. 31	TBD	0%

their chapter binder—policies, procedures, processes, data, committee meeting minutes, and other documentation related to their regulatory standard(s). This workgroup identifies missing, dated, and duplicative policies that are inaccurate and/or inconsistent. The workgroup helps draft and revise policies for leadership approval, and then provides appropriate staff education and training upon full approval. The small workgroups (via their chapter leads or the compliance officer) will share information and bring concerns to the survey readiness committee. Likewise, the survey readiness committee will circle back to the small workgroups about decisions made and further actions needed.

The compliance officer, in coordination with the chapter leads, is key in this communication process.

Additionally, the compliance officer's role in this phase is to manage the SRT by making all updates and noting all progress. The SRT (see Table A) is a robust tool with clearly identified risks, concerns, and opportunities for improvement; specific actions to eliminate risks/concerns or make improvements; clearly established deadlines; and the corresponding status of each item (percent complete). This tool will help facilitate the meetings by focusing on high priority items first, and then all other past due items.

Demonstrated competency and validation checks (3 months)

Upon updating policies, procedures, and practices and receiving necessary trainings, staff are expected to demonstrate competency and knowledge.

The Quality and Compliance staff conduct tracers, audits, and checks on staff competencies/ knowledge to validate that actions are completed, and to ensure continuous compliance and sustained improvements. Moreover, Quality staff collect and

analyze audit data to determine trends and identify other opportunities for improvement. Data should inform leadership about progress and achievements, and also drive decision-making for effective interventions and additional actions. Key tools that are useful in this phase include tracer tools, audit tools, and competency checklists.

In this phase, the compliance officer validates that each binder has updated/accurate policies, procedures, and pertinent documents organized by applicable regulatory standard. How chapters are organized will depend on the size, structure, operations, and type of the facility. As an example, under the CMS standards for hospital and psychiatric hospital, the 12 chapters can be organized in this manner:

1. Emergency Management: 42 CFR § 482.15
2. Food and Dietary: 42 CFR § 482.28
3. Infection Control: 42 CFR § 482.42
4. Governing Body & Leadership: 42 CFR § 482.11, 42 CFR § 482.12, 42 CFR § 482.26, and 42 CFR § 482.27
5. Medical Records, Discharge Planning, & Rehabilitation Services: 42 CFR § 482.24, 42 CFR § 482.43, 42 CFR § 482.56, and 42 CFR § 482.61-62
6. Medical Staff: 42 CFR § 482.22 and 42 CFR § 482.62
7. Nursing Services & Organ, Tissue, and Eye Procurement: 42 CFR § 482.23, 42 CFR § 482.45, and 42 CFR § 482.62
8. Patient's Rights: 42 CFR § 482.13
9. Pharmacy Services: 42 CFR § 482.25
10. Physical Environment: 42 CFR § 482.41
11. Quality Assurance and Performance Improvement Program: 42 CFR § 482.21
12. Utilization Review: 42 CFR § 482.30

Taking action (2 months)

Based on the results of the checks and audits, items are discussed at the next survey readiness committee meeting. Findings from the tracers, checks, and audits are incorporated into the SRT to ensure further actions are implemented and monitored. Oftentimes, performance improvement projects are initiated for more complex corrective actions and long-term efforts. The SRT is a tool that should be used on a continuous, ongoing basis and serve as a roadmap for the facility's compliance efforts. The chapter binders should be maintained year-round, with the identified workgroup and team lead responsible for updating policies and other items as necessary.

Survey performance

During the week of the survey, the facility should structure the survey response team to help manage the following tasks: organize and respond to requests; escort surveyors; take notes; schedule meetings and patient observations; pull data and information; and locate documents and policies. The structure consists of three parts: the command center, survey escorts, and survey scribes.

Command center

The command center is the central room for organizing and coordinating all survey activities during the week of survey. The command center roles are: (1) the command center team lead who has extraordinary organizational skills and the ability to delegate tasks effectively; (2) the command center team members: six to seven staff who are knowledgeable in the electronic health records (EHR) system, can efficiently pull data, have a good understanding of the facility's operations, have familiarity with regulatory standards, and can quickly help make copies and record information; and (3) staff who can interface with surveyors: team members who can help deliver ("run") documents/data to the requested surveyor.

The SRT is a tool that should be used on a continuous, ongoing basis and serve as a roadmap for the facility's compliance efforts.

The command center should be set-up to have the following: (1) a large white board to take down all surveyor requests/tasks; (2) a large wall to post the daily survey schedule; (3) a large table for the command center team to work at and collect data; and (4) a clearly outlined process that defines the steps to be followed for every request:

Table B: Example Survey Task Tracker

REQUESTS					SURVEYOR INFORMATION		COMMAND CENTER	COMPLETION & DELIVERY & NOTES				
NO.	Document or Data Requested	Date/ Time of Request	Patient Name	Unit	Time period	Requesting Surveyor	Staff Escort / Scribe	Staff Assigned	Meeting location	Deadline	Completion date/time	Notes
1	Group Programming	2/1/2019 10:00 AM	Patient A	Unit A	Last 6 months	Ted	Pam / Sue	Liz	Chart Room on Unit A	12 noon	10:30 AM	
2	Interpreter Services-Contracts	2/1/2019 12:00 PM	n/a	n/a	Current	Nancy	Joe / Sandy	Javier	Large Board Room	ASAP	10:45 AM	
3	Treatment Plan	2/1/2019 12:30 PM	Patient B	Unit G	Entire Plan	Kelly	Pam / Sue	Dr. Lee	Chart Room on Unit G	End of Day	11:00 AM	Treatment plan coordinator should review with Kelly

1. All incoming requested are noted on the white board (tasks are tracked and monitored to ensure a quick turn-around time);
2. A specific command center team member will be assigned to collect data/locate documents;
3. A designated internal reviewer will provide a second review of all documents;
4. A copy of the document will be made and recorded on the tracking tool, prior to giving it to the surveyor; and
5. A designated team member will deliver the documents to the surveyor.

The command center maintains the following information throughout the entire survey:

- **Survey Task Tracker** (See Table B): A spreadsheet that reflects the tasks on the white board. This internal document will help the facility clearly understand what the surveyors requested and reviewed during the survey (a powerful tool that will be useful in preparing for all subsequent surveys). Additionally, it is much easier to maintain this list during the survey than to wait until after the conclusion of the survey to try to piece everything together.
- **Survey Schedule** (See Table C): the survey schedule reflects all meetings, facility tours, and unit observations during the week of the survey. This effort allows for effective coordination and proper utilization of resources. Often times, nursing staff are needed in several places and a daily schedule helps coordinate and optimize staff time with surveyors. This also allows the command center to track the location of subject matter experts

Table C: Example Survey Schedule

SCHEDULE						STAFF				SURVEY DOCUMENTS	
NO.	Appointment Day	Time	Condition of Participation Session or Tracer	Condition of Participation Survey Documents	Meeting Room	Staff Lead	Other Staff	Escort	Scribe	Reviewed	Notes
1	Monday, March 1, 2019	9:30 AM	Infection Control Session	Infection Control Binder	Library	Wendy	Dr. Smith	Jin	Sue	Y, Dr. Smith	
2	Monday, March 1, 2019	11:00 AM	Unit Observation	n/a	Unit A	Javier	Dr. Johnson	Rebecca	Sandy	n/a	
3	Monday, March 1, 2019	1:00 PM	Patient Rights Session	Patient Rights Binder	Small Board Room	Dr. Lee	Dr. Smith	Jin	Sue	Y, Joe	

and key staff who are needed ad hoc to review specific documents and participate in patient/staff interviews.

- **Survey binders**: A critical piece to assisting the facility's performance during (unannounced and announced) comprehensive surveys is the preparation of the binders that contain each standard's related policies, procedures, committee meeting minutes, and pertinent documents. With this prepared in advance, the facility avoids massive chaos. If not prepared in advance, staff will require significant time to locate and collect documents in the first two days of the survey.
- **Daily debriefs and final exit debrief**: The daily debriefs are conducted at the end of each day, upon the surveyors' departure. The daily debriefs focus on the high priority items that need immediate attention. Additionally, survey escorts and scribes provide a recap of the day, noting areas of weaknesses, opportunities for improvement, and other concerns. The command center team lead also summarizes the requests, and notes any issues with documents and data. The more comprehensive debrief takes place upon the conclusion of the survey.

Survey escorts

Each survey escort is expected to stay with his/her assigned surveyor at all times. For a survey size of 12 surveyors, seven to eight survey escorts are recommended. The survey escort must have a laptop or cellphone (with texting capabilities) to stay in communication with the command center. The survey escort reports the surveyor's requests to the command center through a central cellphone number or email

address. The command center works on collecting requested data and documents and delivering the information as quickly as possible. The survey escorts are expected to be well-versed with navigating in patient charts and the EHR system. For this reason, escorts are typically staff with clinical background or nursing experience. Additionally, the survey escorts should have experience working with surveyors—limiting conversations and answering questions in a succinct, accurate manner.

Survey scribes

The survey scribes are tasked with taking notes during their time with the surveyor and should be paired with survey escorts. For this reason, a facility should be prepared to have the same number of scribes as escorts. However, the role of the scribe differs in that the survey scribe does not converse with the surveyor, and defers to the survey escort for surveyor's requests and questions. This role serves the purpose of documenting the surveyor process and noting opportunities for improvement/areas of weaknesses. The survey scribe provides feedback to the larger team at the daily debriefs and exit debrief. Most importantly, any issues or findings that require immediate action should be shared, discussed, and immediately addressed in the command center.

Conclusion

Successful survey readiness takes practice, training, and overall cultural change. Staff must work together, in unison, and in the most organized fashion. However, the chief indicator for successful survey readiness is leadership support and guidance throughout the entire process. Leadership plays an important role in establishing a culture that values and fully supports survey readiness efforts.

Acknowledgements

This survey readiness work was a part of a much larger effort—the Systems Improvement Agreement (SIA). The success of survey readiness was directly attributed to the high-performing survey response team and a strong collaboration across the agency with the following key contributors:

- **Anoka Metro Regional Treatment Center (AMRTC) Team:** Rochelle Fischer (Hospital Administrator), Steven Thornton (Deputy Hospital Administrator), Dr. Randy Ward (Medical Director), Dr. Erwin Concepcion (Clinical Services Director), Sharon Dudley (Chief Nursing Officer), Mary Kim (Quality Officer), Rachael Betland (Compliance Officer), and Andy Formantes (Utilization Management Supervisor); in addition to the all the providers and employees of AMRTC who participated in the success of the SIA outcomes.
- **External Consulting Experts:** Dr. Rahul Koranne, Tania Daniels, Tracy Radtke, Jennifer Schoenecker, and Dr. Allison Hong from Minnesota Hospital Association; Debbie Linnes, Nisha Madhavan, and Pamela Brown from DCCS Consulting; and Susan Tabor from Tabor Rx.
- **Direct Care & Treatment Leadership Team:** Marshall Smith (Chief Executive Officer of Health Systems), Dr. KyleeAnn Stevens (Executive Medical Director), Wade Brost (Mental Health and Substance Abuse Treatment Services Executive Director), Derrick Jones (Mental Health and Substance Abuse Treatment Services Chief Operating Officer), Terra Carey (Chief Quality Officer), and Pam Bajari (Mental Health and Substance Abuse Treatment Services Nurse Executive).
- **Department of Human Services Leadership Team:** Shireen Gandhi (Chief Compliance Officer), Amy Akbay (Chief General Counsel), Rick Figueroa (Senior Counsel), Peg Booth (Quality Assurance and Disability Compliance Services Manager), Dr. Daniel Baker (Internal Reviewer), and Lisa Muellner (Registered Nurse); and the support of Commissioner Emily J. Piper and Deputy Commissioner Charles E. Johnson. CT

- Survey readiness should be continuous and operate year-round.
- Survey readiness is a facility-wide effort and requires a team-oriented approach with leadership support.
- Survey readiness requires extraordinary organizational skills and robust tracking tools.
- Facilities should develop a functional command center for the week of the survey to coordinate and track all survey activities.
- Successful survey readiness takes practice, training, and overall cultural change.

New employee orientation

by Frank Ruelas

You arrive at the location where the new employee orientation (NEO) meeting is scheduled. After the current speaker is done, you walk to the front of the room, introduce yourself, and proceed to review your content, which for the most part is exactly the same as the previous NEO meeting, the NEO before that, and so on. Does this description of your participation in the NEO process sound familiar?

This *All Aboard on Compliance* series will share tips that a compliance professional can use to enhance the effectiveness of their efforts in onboarding new members of the workforce, employees' initial exposure to learn of the organization's compliance program, and how it applies to every workforce member's role within the organization.

First impression at NEO

Think of the little things that people might notice when you arrive at the NEO event. Did you arrive late? Did you listen to the speaker before you, or were you busy tapping away on a portable device? Remember, even before you present, you are already on stage in front of your audience.

Do your homework

How much pre-work do you do before you present at each NEO session? Don't be surprised if your response is "none" or if this is a question that you have not previously considered. Find out how to get a roster of attendees a few days before your next NEO event. Often these rosters list each attendee's name, title, role, and other information that can give you useful insight on who is in the audience. You can then work information that's relevant to them into your presentation.

For example, if you are presenting to a group of new workforce members who are in clinical roles, use clinically related situations as examples in your messaging. Using examples or scenarios that your NEO attendees are familiar with may increase the likelihood that attendees will be more engaged and retain the information you are sharing.

Why is this Important

One of your goals at NEO is to provide useful and meaningful information about your organization's compliance program to new workforce members. Doing so in a way that new employees can relate to, while also helping you develop a positive first impression with your audience, can leave a lasting impression that you can be proud of. CT

All Aboard on Compliance *is a new column to address compliance "onboarding" issues to be published in* Compliance Today *through 2019.*

Frank Ruelas

francisco.ruelas@dignityhealth.org) is a Facility Compliance Professional with Dignity Health in Phoenix, AZ.

GOT PRIVILEGE? BEST PRACTICES TO PROTECT PRIVILEGES DURING AN INTERNAL INVESTIGATION

by James Holloway

James Holloway

(jholloway@bakerdonelson.com) is a shareholder in Baker Donelson's Washington, DC office, practicing in the Health/Government Enforcement & Investigations Groups.

Whenever a provider begins an internal investigation into a compliance concern—whether prompted by an employee complaint, a government inquiry, an audit, a media report, or other factors—the protection of legal privileges should be top of mind. Internal investigations typically involve candid and confidential discussions regarding a provider's failure to comply with regulatory requirements, standards of care, or policies. Sometimes there are internal discussions about the provider's awareness of past non-compliance and the failure to take corrective action. There are numerous cases in which a provider was hit with a large verdict or forced into making a large settlement payment, because the government or a private party was able to obtain highly incriminating internal documents that could have been validly withheld from disclosure if the provider had taken the necessary steps to establish and maintain recognized legal privileges. That is an unforced error that providers should strive to avoid.

Common legal privileges for an internal investigation

Two legal privileges are usually available to protect internal investigations. The attorney-client privilege protects written and oral communications that are intended to be confidential between a client and their lawyer, and the privilege applies if a significant purpose of the communication is obtaining or providing legal services. Communications between the provider and its legal counsel during the course of an internal investigation could potentially be protected by the attorney-client privilege. The work product privilege protects materials prepared by or at the direction of a lawyer, for litigation or in anticipation

of litigation. In many cases, an internal investigation is conducted in anticipation of litigation, so the work product privilege may be available.

With any internal investigation, providers should have two related goals in mind. First, establish the privileges for internal communications and materials made during the investigation. Then protect those privileges by avoiding disclosures of information to outside parties that result in a waiver or loss of privileges.

Importance of privileges

Why should providers care about privileges? Because government regulators and plaintiffs' lawyers seeking to extract enormous payments from providers know that the provider's sensitive internal communications and records are likely the best evidence to prove any intentional, willful, malicious, or reckless non-compliance. Although providers may attempt to assert privileges to prevent the disclosure of such information, outside parties that have a financial incentive to push for the information may drag providers into court, where providers will have the burden of proving that privileges apply. Courts scrutinize assertions of privilege and do not hesitate to reject privilege claims that are not valid. In such cases, courts will compel providers to produce the information they attempted to withhold. And the forced disclosure of information that demonstrates a provider's non-compliance may have devastating consequences for the provider.

Therefore, it is critical to establish privileges at the outset of an investigation to make sure that information gathered throughout the course of the investigation is protected. Providers must use a lawyer to assure that privileges apply, so either an in-house or outside lawyer should be involved from the beginning of the investigation. Although a communication with an in-house lawyer may be privileged, a provider's in-house lawyer sometimes functions in a business, non-legal capacity. Similarly, sometimes a provider's compliance officer is a lawyer, and the compliance officer may provide both business and legal services to the provider. In those instances, it may be more difficult to demonstrate that a communication with an in-house lawyer was for the purpose of obtaining or providing legal services on behalf of the provider. The involvement of outside counsel who does not serve a routine business function within the company makes it easier to prove that a significant purpose of confidential communications with a lawyer was obtaining or providing legal services for the provider.

Many internal investigations require the use of outside consultants, such as medical, billing, or accounting experts. Confidential communications with those experts, and the work product of those experts, may be protected by legal privileges if the experts are being used to assist a lawyer in the delivery of legal services to the provider. Thus, the experts should be retained by the provider's lawyer to demonstrate that the experts are working specifically to assist the lawyer with the delivery of legal services.

Misconceptions about privileges

It is important that information is protected by privileges upon its creation, because non-privileged information created during an internal investigation cannot later be converted into privileged information. Thus, a provider that gathers information through its own investigation, before bringing in a lawyer, cannot make the information privileged simply by passing it on to a lawyer who is brought in later during the investigation. Although providers may be tempted to hold off using a lawyer unless and until damaging information is discovered during the investigation, that tactic will not assure that the information is protected by privileges.

...outside parties that have a financial incentive to push for the information may drag providers into court, where providers will have the burden of proving that privileges apply.

There are some other common misconceptions about using lawyers to create privileges. Having a lawyer join a meeting or including a lawyer in an email or memo will not by itself assure a privilege. Likewise, taking a communication between non-lawyers and forwarding it to a lawyer will not assure a privilege. Discussions at a meeting or in an email or memo cannot be protected by the attorney-client privilege unless the discussion involves a lawyer, the communication

is intended to be confidential, *and* a significant purpose of the communication is obtaining or providing legal services. Confidential materials prepared during an internal investigation and later given to a lawyer cannot be protected by the work product privilege unless the material was prepared by or at the direction of a lawyer, either in anticipation of litigation or for a pending litigation. Furthermore, labeling documents as "privileged" will not assure that they are actually privileged. A provider ultimately may be forced through a court proceeding to produce material labeled as "privileged" if it did not meet all the criteria for privileges to apply.

Avoiding waiver of privileges

Once a provider establishes privileges for information gathered during an internal investigation, it is important to avoid a waiver of the privileges through a disclosure of the information. An inadvertent disclosure of privileged information to outside parties may not necessarily waive applicable privileges, but an outside party seeking to obtain privileged information may argue to a court that the disclosure of the information was intentional, not inadvertent. It is not always clear whether a disclosure was intentional or inadvertent. Even when there is a disclosure that the provider believes is inadvertent, there is a risk that a court will determine that it was an intentional waiver of a privilege.

One common risk of waiver is present when email strings are created and forwarded. An initial email communication between a provider's employee and legal counsel may be privileged. However, as the email string grows with additional communications, eventually the email string may be forwarded to a recipient who should not be receiving privileged information, but the person forwarding the email string neglected to notice that an earlier email within the string was privileged. Although labeling an email as "privileged" will not guarantee that it is privileged, such labeling warns recipients of the email that it should be handled carefully because the author considers it to be privileged, which may reduce the risk of waiver from forwarding the communications to unauthorized persons.

The intentional disclosure of privileged information usually results in a waiver of the privilege. Sometimes a provider may consider a voluntary disclosure of privileged information to government regulators as a means to reduce the severity of punishment imposed by the government. There may be valid reasons to disclose privileged information, but it will likely waive applicable privileges. Thus, providers should carefully weigh the pros and cons of disclosure with their legal counsel.

Furthermore, sometimes there are multiple providers involved in an investigation, and they may consider sharing privileged information with one another during the investigation under a joint defense or common interest agreement. Such agreements may be effective to avoid a waiver of privileges, but only if there is an actual common interest among the parties. Using an agreement that merely recites a common interest, when there actually is no common interest among the parties, will not assure that privileged information can be shared without a waiver. Because there is a risk that sharing privileged information with another party may not necessarily be protected by a joint defense agreement, providers should consult with legal counsel to evaluate whether a joint defense agreement will effectively protect the sharing of privileged information in a provider's particular circumstances.

Conclusion

Providers conducting an internal investigation are entitled to assert valid legal privileges, but they must act carefully, in consultation with legal counsel, to assure that privileges are established and preserved throughout the investigation. CT

- Be sure to have in-house or outside counsel lined up at the start of an internal investigation.
- Legal counsel should retain the experts who will be assisting with an investigation.
- Label materials as "privileged" to alert recipients to safeguard the materials, but do not expect that label to protect non-privileged information.
- Be careful when forwarding or sharing privileged information to avoid waiving privileges.
- Disclosing privileged information outside the company should only be considered after consulting with legal counsel.

Remembering Jesse

by Kelly M. Willenberg

In 1999, Paul Gelsinger's 17-year-old son Jesse was suffering from a genetic disease called ornithine transcarbamylase deficiency. A buildup of ammonia was making Jesse very sick from dietary choices, including a strict non-protein diet. A carefully followed diet and medication controlled the disease. Given an opportunity to participate in a gene therapy trial designed to test possible treatments for his disease, Jesse decided that when he turned 18, he would give consent. The trial would use gene therapy or an adenovirus to transport a normal gene into his liver. For the most part, Jesse was informed that subjects who had received the adenovirus had not had serious complications. But a mere four days after the gene therapy, Jesse suffered an immune reaction and died.

Last fall, I met Jesse's dad at a conference where we were both speakers. Listening to this father describe what his family went through inspired me to consider the research compliance profession and where we are today. Jesse's family felt that Jesse had not been properly informed. Later they discovered that adverse reactions were not reported or communicated. There were questions of conflicts of interest and data not being reported properly. Today we are moving from gene therapy and proton therapy to customized molecular profiling for treatment—all of which began in a clinical trial. Oversight, safety concerns, and evaluation are top priorities in the planning and carrying out of clinical research and must not be taken for granted. Research compliance is needed and should be first and foremost in all settings.

Remembering the ethical side of why patients consider participating in a clinical trial, and how compliance oversight protects that sacred agreement, is the reason we are in the careers we are in today. Clinical research has changed over the nearly 20 years that have gone by since Jesse Gelsinger's death. But we must remain diligent in the role of a research compliance professional and not take for granted why that role is important.

In corresponding with Mr. Gelsinger since the day I met him, I asked him what one thing he would like all research professionals to consider in the important role they play. He said, "Keeping everyone as safe as possible in research can only be accomplished through protocol compliance and by adapting what Jesse demonstrated: Do what you do, not for recognition, nor for money, but only to help. Only then will you get research right, and have a blameless prosperity." CT

Kelly M. Willenberg
DBA, RN, CCRP, CHRC, CHC
(kelly@kellywillenberg.com)
is President and CEO of
Kelly Willenberg, LLC in Chesnee, SC.

PAYMENT COLLECTION CONTROLS

by Darryl Rhames

Darryl Rhames
CFE, CICA
(drrhames@hotmail.com) is Director of Compliance Auditing at the University Health System in San Antonio, TX.

Payment collections are the beginning of the revenue cycle. Some may view this as a no brainer or immaterial subject matter. However, have you ever taken a look at your total cash, credit card, and check collections? Have you compared that monetary value versus how much you bill out, due to not collecting co-pays or not being set up to collect payments when patients can pay right now?

What if you went to a grocery store and they told you, "Don't worry about paying for the groceries at this time; we'll bill you for them." What percentage of people would take the goods and make sure they settle the bill later? No way are grocery stores doing that! They want their money as soon as you are ready to check out. They ensure they collect money on every transaction. Why shouldn't you do the same at your facility or at least be set up to do the same? Could you imagine what collecting on every transaction would mean for your company? Think of what processes you could improve, the investments you could make, the repair or renovations you could complete, the impact to patient care, etc.

Now are payment collections starting to become more important to you? Well, in healthcare, cash is still very relevant as a payment method. Yeah, I know. Cash...really...that is a dying tender. Is that a true statement? Not at all. It depends on where you are that determines how widely cash is used as a major form of tender. Credit or debit card usage normally surpasses cash, but does that mean you shouldn't accept cash? Of course not. I have never heard of a service fee for accepting cash. MasterCard, Visa, American Express, and Discover don't get a cut of a cash payment. Ironically, it costs less to accept cash. So, it was decided to accommodate all forms of payment at every hospital campus and clinic.

Reflecting back on payment collection

More than 100 years ago, services were being provided to patients in hospitals, and patients were paying for their care. Over the course of history, hospitals developed:

- Cashier offices to accept multi-tender payments
- Patient service cashiers to register patients and collect copays
- Retail service cashiers to handle food or gift purchases for patients and their visitors

Outside of cash, credit card, and checks, hospitals set up payroll deduction options for employees to ensure funds were collected immediately for cafeteria food or hospital services.

It sounds like all areas can collect; however, where there are collections, there are also chances of loss.

What do I mean? Fraud, theft, abuse, and waste

There is a saying: If you can't protect it, don't collect it!

Once it was decided to accept multiple forms of payment (e.g., cash, check, credit cards) across all clinics, a need to protect the collections arose. What would be done to regulate payment collections and ensure proper internal controls were in place to reduce loss or fraudulent activity? A committee was formed by the efforts of the departments of Auditing and Compliance. The committee consisted of key personnel, such as vice presidents, directors, and managers, from both the patient services (clinics/hospital) and the retail service areas (cafeteria, patient trays, gift shop) to come up with rules and regulations for payment collections. During these committee meetings, basic competencies were developed, outlining what cashiers needed to know and what procedures should be in place to ensure all collection operations ran appropriately. A payment collections handbook was developed for all cashiers to abide by. A discipline grid was also developed to guide managers on what consequences were warranted for procedural errors, incomplete reconciliations documentation, and overages and shortages.

As time passed, this handbook was updated to remain relevant as the collection avenues increased. As a part of the compliance program, mandatory training was developed to certify all employees whose jobs included payment collection. Surprise cash audits were being conducted to review cashier activity, and surveillance cameras were installed to capture payment activities. Additionally, incentive pay was established for people collecting payments on the patient side.

Standardization for collecting payments

Now that you have the background or reasons behind establishing policies and procedures around payment collections, here are the phases or objectives used to begin establishing standardization for payment collections.

Phase 1

The first phase encompassed capturing financial information, including the identification of all collection points and a review of the pros and cons to make the collection more successful. For example, at the front-end (e.g., admissions, registration, mobile units, and pharmacy) are areas where patient services cashiers are placed in clinics. Usually these positions are called upon to ensure the accuracy of the patients' demographic information, personal identity information, and to collect payments. Although traditionally the least paid positions, the accuracy of patient data and collection of co-payments starts with them. Phase 1 also involves setting up internal controls to ensure the accuracy and reliability of captured financial information, including patient payments from satellite clinics/hospital services, and retail sales for nutritional services.

Once it was decided to accept multiple forms of payment (e.g., cash, check, credit cards) across all clinics, a need to protect the collections arose.

Comparably, on the retail side, the retail service cashiers are stationed at point-of-sale registers, and are lower paid positions; however, the accuracy of merchandise sales and collection of payments (purchases) starts with them.

Phase 2

Once the collection points were identified, next was to established procedures to establish accountability and provide the tools and safeguards

to protect the systems monetary collections or assets. This involves implementing physical and system controls to safeguard assets, such as setting up a payment collection point for clinical front desk operations and retail cashier locations (e.g., cafeteria and gift shop).

Phase 3
The adoption of meaningful training for registration clerks and cashiers, including:

- Mandatory training programs to educate employees;
- Deciding which departments should be involved in the training of personnel responsible for payment collections;
- Development of policies and procedures, payment manuals, or guides;
- Standardized disciplinary actions for overage and shortages of funds; and
- Development of payment collection tool kits.

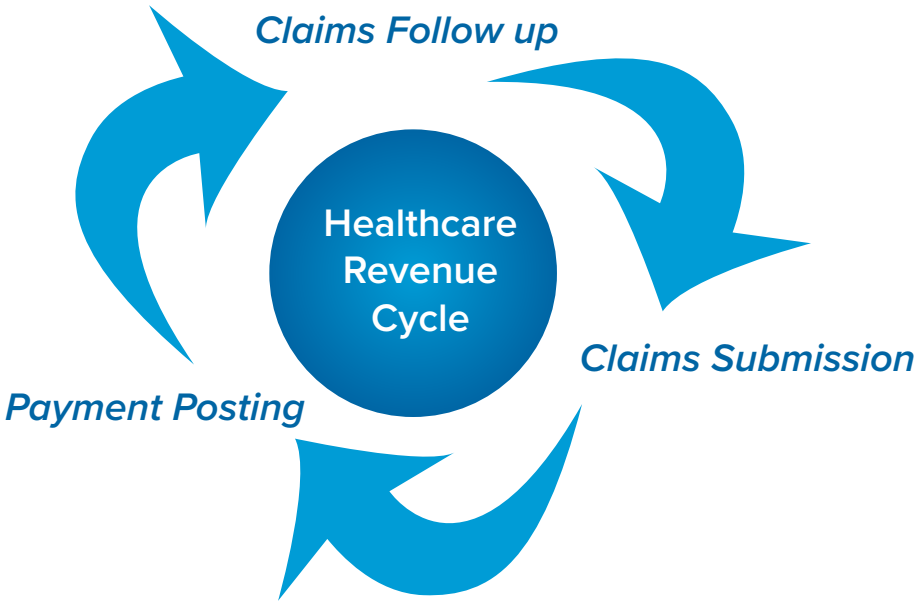
Phase 4
Next came the development of practical suggestions to detect and prevent fraud in a payment/cash collection environment (e.g., front desk operations and admissions), including retail operations (e.g., cafeteria and gift shop) and the cashier's office, and detection tools for counterfeit money.

The training program

To begin the second phase, a collection walk-through process was established along with revamping the mandatory training program for the retail cashiers and clinical front desk personnel. For the mandatory training class, the staff must pass an online exam. The cashier was required to obtain a payment collection certificate as a prerequisite to collecting payments. The training class covers:

- Managing, securing, posting, reconciling, balancing, and depositing collections;
- Authentication of cash (*www.newmoney.gov* or *www.uscurrency.gov*);
- Identifying fraudulent checks and meal vouchers;
- Processing and recording refunds (e.g., co-pays, "no service" slips). The cashier can return a check, refund cash, or refund the credit card if the patient did not receive services. In order to process a refund, the cashier must obtain a completed no service slip from the patient's healthcare provider.
- Voids, "no sale" key usage, deleting transactions, management oversight; and
- Out-of-balance procedures and consequences.

At first, this training was only a part of the compliance training program, where the training was requested and then provided. To encompass the entire organization on a standard routine for payment collections training, a company-wide training was being provided for all front-desk personnel on a standard monthly schedule. Because this was already in place, the system would incorporate collections setup and training orientations with clinical front-desk training led by instructors from Information Technology (IT), Admissions, Billing, and me from Integrity Services. We trained on the payment systems and explained how the cashiers initiate the revenue cycle and ensure accuracy, from payment collections to payment posting.



Walk-through process

The next part of the second phase was establishing collection setup walk-throughs prior to approving an area to collect payments. To establish the walk-through process, I considered the questions below and started the process:

- Cashiers and front desk personnel are trained, but what

did we need to review about the clinic or cafeteria they work in regarding payment collection?

Questionnaires were developed to assess what was needed to secure collections and prevent theft/fraud. The questionnaires asked questions regarding:

- Cameras/surveillance
- Electronic badge readers
- Safe installation/location
- Lock boxes
- Locked draws and doors
- Separation of duties throughout the collection and reconciliation process
- How much cash was kept on hand
- Who was the custodian of the cash
- Was an armored truck pickup or secured escorts needed for making deposits or getting change
- Renovations or new construction needed for patient and staff safety
- What was needed to accept multiple forms of payment (e.g., credit cards, checks, cash, online)

Additionally, if possible, involvement during construction was preferred. During these walk-throughs, our police department, IT, and Financial Accounting were involved, so all concerns could be voiced. In conjunction with these areas, once a walk-through was completed, I drafted a summary on behalf of the Compliance department and sent the correspondence to the vice president and director of the area. The summary included recommendations for payment collections and the cost associated with becoming compliant.

These walk-throughs also helped to assess and set up controls that enabled the areas to safeguard their funds and prevent, deter, and detect both errors and fraud. Implementing the recommendations would help to ensure receipts and disbursements are appropriately received and accounted for.

...consistent consequences for procedural errors and over/short variances help deter rule infractions. The offender ponders whether the act is worth the consequence.

During the walk-throughs, I aimed to identify key controls over cash handling with the following questions:

- **Are proper separation of duties and verification of collections** (e.g., random audits, checking for accuracy) **present?** Separation of duties ensures an appropriate division of responsibilities that serves as a cross-check for cash handling duties and enhances the chance of detection, because more than one person is involved in the process.
- **Are collections being verified?** Verification or reconciliation involves ensuring what was recorded was actually received. This is the review process for accurate collections.
- **Is there a consequence for violation of collection policy?** Implementation of consistent consequences for procedural errors and over/short variances help deter rule infractions. The offender ponders whether the act is worth the consequence.
- **Does the video surveillance work or is it just a decoy?** Review video surveillance of collection areas randomly, and make sure staff knows the cameras are recording. Offenders tend to be more conscious of their actions when they know people are watching the cameras.

Manuals and toolkits

To further assist staff with this training initiative, the manuals and toolkits developed were placed on our department's website. The content included:

- **Online handbooks for patient and retail cashiers** that contained the requirements for the certified cashier designation and competencies. Every cashier was made aware that they were responsible for knowing the information in the handbooks to maintain their designations.
- **Calendars** that listed training dates to register online to attend training sessions.
- **Logs** to use for counting the safe, verifying, change funds, etc.
- **Lock box memos** that explained proper lock box protocol.
- **Surprise audit checklist** of what to look for.
- **Cash collection guidelines**, which contained the discipline grid of consequences for policy violations.
- **Education materials on authentication of U.S. currency** for detecting counterfeit currency.

The methods in which we collect payments are constantly evolving (e.g., mobile pay, online payment via credit card and bank accounts [Automated Clearing House or ACH], advanced credit card terminals) and these options must be considered and incorporated in the training as well. As a result of the training on payment collections and increasing the amount of cash collected, the standardization of the payment collection process was recommended to be a part of a 100-day-lean project. The components of the lean project include strategy alignment, visual management, standard work, continuous improvement problem solving, and leadership standard work exercises. This is an area that is supported heavily by senior leadership.

Based on the recent discussions, we will reboot the training provided and add additional features to our website that are more robust and interactive in regard to:

- Outlining the entire process from payment approval walkthrough requests,
- New collection questionnaires,
- Updated training manuals,
- Revised policies and procedures, and
- Designated points of contact for payments collection walk-throughs (i.e., Compliance, Internal Audit, Law Enforcement, Information Technology, Financial Accounting, Facilities Management, and Maintenance)

Connect with me via the HCCA community if you have any questions about starting or revising your payment collections and payment protection program. CT

- Ensure accuracy and reliability of captured financial information.
- Implement physical and system controls to safeguard assets.
- Develop a company-wide training program.
- Create audit tools, such as questionnaires, to monitor payment activity.
- Use walk-throughs to help detect and prevent fraud.

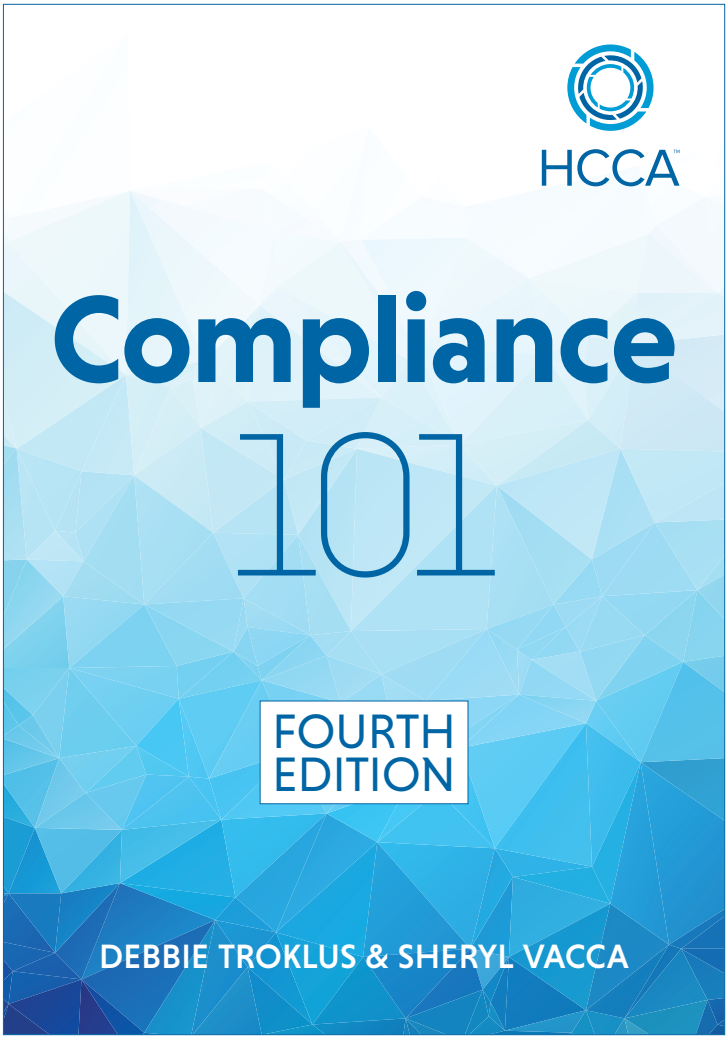
Portable job training

Compliance 101

FOURTH EDITION

Authors Debbie Troklus and Sheryl Vacca have updated *Compliance 101* with changes in federal regulations, including HIPAA, HITECH, and the Omnibus Rule as well as new insights on what it takes to build an effective compliance program. This book reviews the fundamentals in healthcare compliance, including the seven essential elements of a compliance program.

This book is ideal for compliance professionals new to the field, compliance committee members, compliance liaisons, board members, and others who need a foundation in compliance principles.



Features:

- Step-by-step instructions on setting up and maintaining a compliance program
- A chapter dedicated to HIPAA privacy and security regulations
- A glossary with compliance terms and definitions
- Sample compliance forms and policies

hcca-info.org/compliance101

HCCA
Health Care Compliance Association

NEW CMS RULE REVISIONS AFFECTING YOUR INPATIENT REHABILITATION FACILITY

by Danielle C. Gordet

Danielle C. Gordet,
JD, MPH, CHC
(dgordet@gmail.com) is a Director of Compliance in the Office of Compliance & Ethics, at Jackson Health System, in Miami, FL.
in /in/danielle-gordet

An inpatient rehabilitation facility (IRF) must meet specific coverage criteria for care to be considered reasonable and necessary. Failure to meet the IRF coverage criteria may result in denial of a claim. Because the IRF coverage criteria had not been updated since January 1, 2010, the Centers for Medicare & Medicaid Services (CMS) realized that changes were needed to maximize the quality of care provided to IRF patients. Therefore, beginning fiscal year 2019 (for all IRF discharges on or after October 1, 2018), CMS implemented revisions to the IRF coverage criteria in an effort to "allow providers and physicians to focus the majority of their time treating patients rather than completing paperwork."

These revisions were published on August 6, 2018, as part of CMS's IRF Prospective Payment System final rule (IRF final rule). The changes were aimed at alleviating the administrative burden placed on IRFs. This article will outline the revisions to the IRF final rule regarding coverage requirements and will provide recommendations to help you ensure compliance at your IRF.

Physician supervision

IRF coverage criteria require that at the time of the patient's admission to the IRF, there must be a reasonable expectation that the patient "requires physician supervision by a rehabilitation physician." To satisfy this requirement, the rehabilitation physician must conduct at least three face-to-face visits with the patient per week throughout the patient's stay in the IRF.[1] These face-to-face visits must be documented in the patient's medical record.[6]

The purpose of the physician supervision requirement is "to ensure that the patient's medical and functional statuses are being

continuously monitored as the patient's overall plan of care is being carried out."[2] CMS believes that the physician supervision requirement's purpose is different from that of the post-admission physician evaluation (PAPE), which must be completed by a rehabilitation physician within 24 hours of the patient's admission to the IRF and be retained in the patient's medical record.[1] The purpose of the PAPE "is to document (in the IRF medical record) the patient's status on admission, identify any relevant changes that may have occurred since the preadmission screening, and provide the rehabilitation physician with the necessary information to begin development of the patient's overall plan of care."[2]

CMS has reiterated its belief that the physician supervision requirement and the PAPE are two different types of assessments; however, in the IRF final rule, CMS modified the physician supervision requirement to allow the PAPE to count as one of the face-to-face physician visits. [7] This revision will allow the rehabilitation physician "the flexibility to assess the patient and conduct the post-admission physician evaluation during one of the three face-to-face physician visits required in the first week of the IRF admission."[2] It should be noted that this revision is not meant to limit rehabilitation physicians from seeing patients more than three times in the first week of the patient's IRF stay.[7]

CMS expects "that each rehabilitation physician will exercise his or her best clinical judgement to determine the need and frequency of rehabilitation physician visits for a given patient." Interestingly, CMS estimates that only about half of IRFs will actually adopt this new policy, because many rehabilitation physicians visit patients more than the minimum three times per week.[7]

Recommendation: Provide education to the providers at your facility to ensure that they understand the requirements for PAPEs and physician supervision, including the importance of adequate documentation in the medical record. Physicians must remember that the PAPE requirement remains unchanged; however, by adequately completing and documenting the PAPE, a physician is only required to have two additional face-to-face visits with the patient in the first week of the patient's admission to the IRF.[7]

Interdisciplinary team meetings

Another IRF coverage requirement is that the patient's care must be managed by an interdisciplinary team, which includes weekly team meetings that satisfy the requirements specified in the regulation. The requirements state that "team meetings must be led by a rehabilitation physician and that the results and findings of the team meetings, and the concurrence by the rehabilitation physician with those results and findings, are retained in the patient's medical record."[7]

CMS understands that a rehabilitation physician might not be able to attend all the team meetings in person; therefore, CMS has previously instructed physicians that the rehabilitation physician may attend the team meetings by telephone "as long as it is clearly demonstrated in the documentation of the IRF medical record that the meeting was led by the rehabilitation physician."[8]

In the IRF final rule, CMS revised this requirement to include the option for the rehabilitation physician to lead the team meetings "remotely via another mode of communication, such as video or telephone conferencing." [1,9]

Additionally, in the IRF final rule, CMS explicitly states that it is finalizing this rule without any additional documentation requirements, because it does not "feel that documentation of the rehabilitation physician's physical location during the team meeting in the IRF medical record is needed to ensure that the rehabilitation physician is making the decisions."

...in the IRF final rule, CMS modified the physician supervision requirement to allow the PAPE to count as one of the face-to-face physician visits.

CMS anticipates that this revision "will allow time management flexibility and convenience for all rehabilitation physicians, especially those located in rural areas who may need to travel greater distances between facilities." In the future, CMS may allow other team meeting attendees to participate remotely; however, for the time being this new revision only applies to the rehabilitation physician.[8]

By implementing this revision, CMS has given IRFs the flexibility to: (1) adopt the new rule and allow

the rehabilitation physician to participate in the team meetings remotely; (2) maintain a protocol that the rehabilitation physician must lead the team meetings in person; or (3) allow the rehabilitation physician to participate in the team meetings remotely during certain situations, such as only allowing remote participation during extenuating circumstances.[8]

CMS maintains the belief that the majority of the IRF visits should be face to face to maximize the quality of care provided to a patient...

Recommendation: Work with the leadership at your IRF to decide whether rehabilitation physicians will be permitted to participate remotely when conducting the team meetings and, if so, under what conditions. Based on your IRF needs, you may have a preference for one approach over another. For instance, your IRF may have a very high functioning, in person, team meeting protocol already in place that you do not want to disrupt. If that is the case, it may be best for your IRF to establish a policy that requires the rehabilitation physicians to be physically present for the team meetings.

Admission order documentation

In the IRF final rule, CMS removed the requirement that at the time of patient admission "the inpatient rehabilitation facility must have physician orders for the patient's care during the time the patient is hospitalized."[10] The purpose behind removing this requirement was to reduce regulatory redundancy and administrative burden, because the requirement for an admission order continues to be addressed through hospital Conditions of Participation and hospital admission order payment requirements.[11] For instance, CMS considers an individual to be a hospital inpatient if the patient is formally admitted under an order for inpatient admission by a physician or other qualified practitioner.[9] Qualified practitioners (other than physicians) may be permitted to order the inpatient admission, if they are allowed to do so under "State law, including scope-of-practice laws, hospital policies, and medical staff bylaws, rules and regulations."[12]

In addition to removing duplication in the IRF coverage criteria, CMS also implemented a change under the Hospital Inpatient Prospective Payment Systems final rule. CMS removed the requirement that as a *condition of payment*, the "physician order must be present in the medical record and be supported by the physician admission and progress notes, in order for the hospital to be paid for hospital inpatient services." CMS will consider this requirement satisfied if "other available documentation, such as the physician certification statement when required, progress notes, or the medical record as a whole, supports that all the coverage criteria (including medical necessity) are met, and the hospital is operating in accordance with the hospital conditions of participation."[13]

To be clear, this change does not alter the requirement that "a beneficiary becomes an inpatient when formally admitted as an inpatient under an order for inpatient admission (nor that the documentation must still otherwise meet medical necessity and coverage criteria)." It only revises the prior documentation requirement that inpatient orders must be present in the medical record as a condition of payment.[14]

Recommendation: Continue to ensure that inpatient orders are entered in accordance with CMS regulations. "The physician order remains a significant requirement because it reflects a determination by the ordering physician or other qualified practitioner that hospital inpatient services are medically necessary, and initiates the process for inpatient admission."[13]

Potential future changes

CMS is considering whether rehabilitation physicians should have the flexibility to conduct some IRF patient visits remotely via other modes of communication, such as video or telephone conferencing.[11] As discussed earlier in this article, the current IRF physician supervision requirement necessitates that the rehabilitation physician conduct at least three face-to-face visits with the patient per week throughout the patient's stay in the IRF.[1] In 2010, when the IRF coverage criteria were initially implemented, CMS included this face-to-face requirement "to ensure that the patient receives the most comprehensive in person care by a rehabilitation physician throughout the IRF stay." CMS maintains the belief that the majority of the IRF visits should be face to face to maximize the quality of care provided to a patient; however, given the advent and quality of alternative methods of communication, CMS is considering giving rehabilitation physicians more flexibility in

conducting patient visits. CMS is not ready to implement changes to the three face-to-face requirements at this time, but may do so in the near future.[11]

CMS is also contemplating whether the current IRF requirements should be modified to allow non-physician practitioners (e.g., physician assistants and nurse practitioners) to play a greater part in the IRF care, thus removing some of the burdens placed on rehabilitation physicians (e.g., face-to-face visits and accompanying documentation). CMS has not yet modified these requirements due to concerns regarding whether non-physician practitioners have the specialized training required to handle these responsibilities. CMS also has concerns that implementing any changes to these requirements may impact patients' ability "to receive the hospital level and quality of care that is necessary to treat such complex conditions." CMS will continue to contemplate this potential refinement to current IRF coverage criteria and may make changes in the future.[11]

Conclusion

CMS has made an effort to alleviate the regulatory burden placed on IRFs, in part, by making changes to IRF coverage criteria. Interestingly, many of the changes that CMS implemented are optional. For instance, the rehabilitation physician may conduct the interdisciplinary team meetings remotely, but he/she is not required to do so.[8] Similarly, although the PAPE may count as one of the three face-to-face requirements, the rehabilitation physician has the flexibility to visit the patient more than three times in the patient's first week of IRF admission.[2]

Each IRF should evaluate the changed criteria, decide how they would like to address the changes, and establish processes to implement those changes, if any. Once this has been done, the IRF should ensure that it provides its personnel with the appropriate training. Remember that even though CMS has loosened a few of the previous IRF requirements, the majority of them remain the same and must be followed. CT

The views expressed herein are those of the author and do not necessarily reflect the views of Jackson Health System. The information contained herein is not intended to convey or constitute legal advice and is not a substitute for consulting a qualified attorney. You should not act upon any such information without first seeking qualified counsel on your specific matter.

Endnotes

1. 42 CFR 412.622 (Basis of payment). https://bit.ly/2Nv9rFH
2. 83 Fed. Reg. 38514, 38550 (Inpatient Rehabilitation Facility Prospective Payment System for Federal Fiscal Year 2019) August 6, 2018. https://bit.ly/2A7HBta.
3. 83 Fed. Reg. 38514, 38549.
4. 83 Fed. Reg. 38514, 38514.
5. Centers for Medicare and Medicaid Services, *Medicare Benefit Policy Manual*, CMS Pub. 100-02, Chap. 1, Sec. 110 (Rev. 234, March 10, 2017). https://go.cms.gov/2TubP2r
6. Danielle C. Gordet, "Rehabbing critical documentation processes in your inpatient rehabilitation facility," *Compliance Today*, September 2018, Volume 20, Issue 9, p. 77.
7. 83 Fed. Reg. 38514, 38551.
8. 83 Fed. Reg. 38514, 38552.
9. 83 Fed. Reg. 38514, 38553.
10. 42 CFR 412.606 (Patient assessments). https://bit.ly/2BlQkd8
11. 83 Fed. Reg. 38514, 38554.
12. 42 CFR 482.24 (Condition of Participation: Medical Record Services). https://bit.ly/2KjUk0J
13. 83 Fed. Reg. 41144, 41507 (Hospital Inpatient Prospective Payment Systems for Federal Fiscal Year 2019), August 17, 2018. https://bit.ly/2QcjrrE
14. 83 Fed. Reg. 41144, 41510.

- The post-admission physician evaluation may count as one of the three face-to-face physician visits in the first week of a patient's inpatient rehabilitation facility (IRF) admission.
- The rehabilitation physician may now lead the interdisciplinary team meetings remotely via video or telephone conferencing.
- CMS removed the IRF admission order documentation requirement; however, to be considered an inpatient, a patient is still required to be formally admitted as an inpatient under an order for inpatient admission.
- CMS is considering future policy changes that would give rehabilitation physicians the flexibility to conduct some IRF patient visits remotely.
- In the future, CMS may allow non-physician practitioners to play a greater role in IRF care, thereby removing some of the requirements placed on rehabilitation physicians.

PHYSICIAN COMPENSATION ARRANGEMENTS: ROBUST REVIEWS ARE A MUST

by Tynan O. Kugler and Susan Thomas

Tynan O. Kugler

Susan Thomas

Tynan O. Kugler *(tkugler@pyapc.com) is a principal, and* ***Susan Thomas*** *(sthomas@pyapc.com) is a manager at PYA headquartered in Knoxville, TN.*

Negotiating physician compensation arrangements has become more prevalent as an increasing number of physicians are employed by, or contract with, health systems, hospitals, and healthcare facilities to provide various services. Such arrangements are often complex, with multifaceted compensation, production, and quality-related elements, making them subject to hard-hitting regulatory scrutiny. Therefore, it is vital that hospital and health system executives implement robust contract management systems to assure the arrangements are negotiated in compliance with regulatory guidelines. Further, all involved parties should ensure that the supporting documentation adequately substantiates contract provisions for the defined arrangement.

The burden to make certain that physician arrangements are compliant with regulatory and legal considerations can be overwhelming. Violations of the Stark Law (Stark), Anti-Kickback Statute (AKS), or the False Claims Act (FCA) can not only be costly, but also embarrassing to a health system, its physicians, and its executives—potentially causing long-lasting reputational damage and distrust. In recent years, several hospitals have paid massive penalties, ranging from $25 million to $115 million, for excessive or improper physician compensation arrangements that exceeded fair market value (FMV) and may not have been commercially reasonable.[1]

For this reason, health system executives must recognize the need for conducting a thorough review of physician arrangements on a regular basis. Organizations will be in a stronger position if physician compensation arrangements are a fundamental component of their compliance work plans. Many potential compliance violations can be mitigated—or even prevented—by completing regular, detailed compensation arrangement reviews.

Physician compensation arrangement tracking may not be a top priority for some organizations, given limited resources and competing concerns. This is complicated by the fact that an organization's management of such arrangements may be decentralized or, in larger systems, perhaps maintained by external parties including legal

counsel. However, comprehensive contract review and management is essential to ensure that the arrangements are current and meet organizational and regulatory requirements. Analyses of physician arrangements can reveal complicated party relationships, which could bring legal challenges. Furthermore, the executed contracts may often contain unintentionally vague language.

These issues can lead to uncertainty and a misunderstanding of the arrangement, inadvertently creating situations that otherwise could have been mitigated if thoroughly and proactively addressed. Physician compensation arrangements are often multifaceted—covering multiple services in a single arrangement, which can significantly impact FMV and commercial reasonableness. Commercial reasonableness is defined by the Stark Law as:

> An arrangement will be considered 'commercially reasonable' in the absence of referrals if the arrangement would make commercial sense if entered into by a reasonable entity of similar type and size and a reasonable physician (or family member or group practice) of similar scope and specialty, even if there were no potential DHS [designated health services] referrals.[2]

Increased scrutiny

As the aggregate number of physician compensation agreements increases so, too, does regulatory oversight. Federal statutes, such as Stark, AKS, and FCA, directly affect physician employment or contracts for services, as do some state laws. Steep penalties can be imposed for noncompliance, particularly related to financial relationships with physicians.

Stark prohibits referrals for healthcare services amongst physicians and the entities with which they have financial relationships, unless the arrangement is structured to fit within a regulatory exception. Sanctions include repayment, fines, and exclusion from federal healthcare programs.

AKS prohibits the exchange of, or offer to exchange, anything of value that may influence the referral of federal healthcare program business. Criminal and civil penalties can be levied against any individual or entity that knowingly and willingly offers, pays, solicits, or receives any remuneration—including any kickback, bribe, or rebate—directly or indirectly, overtly or covertly, in cash or in kind, to any person to induce referrals, or to purchase, order, or lease an item.

FCA places liabilities on companies and individuals who attempt to defraud federal programs. It prohibits any person from knowingly presenting, or causing the presentation of, a fraudulent claim for payment to a federal healthcare program. The FCA has become an important, if not *the* most important, governmental tool for demanding healthcare providers' compliance with the requirements of federal healthcare program participation. Under the FCA, hospital or physician service payments that violate Stark or AKS are considered fraudulent. The FCA creates liability for any individual who knowingly uses or submits (or causes to be submitted) a false record, statement, or claim for payment to the government. Proof of intent to defraud is not required.

Steep penalties may also result from lack of compliance with various other certifications as the content identified within physician arrangements is central to completion of other critical governmental documentation. For example, certification requirements for Medicare cost reports must be taken into consideration. The misrepresentation or falsification of any information in a cost report may be punishable by criminal, civil, and administrative action, as well as a fine or imprisonment.

Many potential compliance violations can be mitigated—or even prevented—by completing regular, detailed compensation arrangement reviews.

Specifically, the Medicare cost report includes facility costs associated with physician administrative time (Part A) and physician patient treatment time (Part B). The Centers for Medicare & Medicaid Services (CMS) expects that physician compensation agreements entered into by hospitals and health systems appropriately allocate the compensation between the administrative and professional components. Specifically, all physician time is defaulted to

The Department of Justice's focus on individual accountability leaves little doubt that efforts to assert individual accountability extends to officers and executives...

Part B, unless documentation shows the time qualifies for Part A. To report allocation of physician compensation, all compensation must be identified and quantified. Next, documentation must be reviewed to segregate Part A from Part B. Part A is reimbursable on the cost report and must be documented and verified with time studies, timely attestation signatures, and implementation of contracts.

Compliance with filings and the aforementioned laws has increasingly taken center stage as oversight agencies, such as the Department of Health and Human Services Office of Inspector General (OIG), have reinforced their goal to reduce healthcare fraud, waste, and abuse. Several dedicated entities have stepped up efforts to combat healthcare fraud, including the Medicare Fraud Strike Force, the FBI Healthcare Fraud Prevention Partnership, the IRS Healthcare Fraud Criminal Investigation Unit, the OIG Health Care Fraud Prevention and Enforcement Action Team, and the USPS Office of Investigations Healthcare Provider Fraud Unit.

Such agencies are increasingly pursuing allegations against individual physicians and other providers, not only the hospitals and other organizations that employ them. These actions serve as reminders that physicians are increasingly held accountable for arrangements that may be in violation of multiple federal laws. As such, healthcare organizations that employ and/or contract with physicians must hold physicians accountable for regulatory compliance as part of the compensation arrangement to limit the organization's exposure to risk. The consequences of physician noncompliance can be severe.

Examples of these agencies' recent significant legal actions involving physician conduct are:

- July 2017: $1.3 billion in false billings to Medicare and Medicaid related to joint injections, opioid prescriptions, and drug screenings;[3]
- November 2017: $6.6 million in fraudulent claims to Medicare for nonemergency transports of dialysis patients;[4]
- January 2018: $2 million in restitution and four years in prison for a home health kickback and identity theft scheme;[5]
- February 2018: $63 million false billing for partial hospitalizations involving a community mental health center;[6] and
- March 2018: $30 million for pharmacy marketers who paid physicians to write prescriptions for expensive topical compounded medications.[7]

In addition, executives and members of boards of directors may potentially be held responsible for any organizational noncompliance.[8] The closer alignment of hospitals and physicians under new models of care delivery requires greater board oversight of compensation arrangements. The Department of Justice's focus on individual accountability leaves little doubt that efforts to assert individual accountability extends to officers and executives who "lead or participate" in activities perceived to be illegal conduct.

Goals of a review

In most healthcare organizations, physicians represent the highest paid group of employees. As such, healthcare organizations must develop and implement a robust review process of all physician compensation arrangements to ensure such contracts comply with regulatory and policy requirements. This review process serves to provide oversight of increasing integration of services and financial relationships with physicians, while helping to mitigate aggressive government enforcement efforts, unyielding penalties, and organizational risk.

The objectives of physician arrangements or contracts review are numerous and may include, but are not limited to:

- Gaining an overview and oversight of organization-wide contracting practices;
- Uncovering potentially noncompliant arrangements (or that have become noncompliant over time), bringing them to the attention of the compliance officer, the Legal Services department, and other appropriate internal and external parties;

- Examining compensation to assure consistency with FMV and commercial reasonableness;
- Ensuring that all arrangements have the necessary, accurate supporting documentation;
- Evaluating a system for duplicative services and agreements; and
- Determining whether contract management systems are complete and appropriately maintained.

Multiple types of physician compensation arrangements may be necessary for healthcare organizations, including, but not limited to:

- Employment
- Professional services
- Income guarantee or support
- Loan repayment
- Recruitment
- On-call pay
- Joint ventures
- Administrative positions
- Co-management services
- Facility and equipment leasing

Delineate a robust review process

A solid and robust compensation review process is needed to address the complex risks and challenges in physician arrangements.

The team

For the review process to be efficient and successful, a competent and trained team should be appointed, preferably including those who have experience conducting contract evaluations. A specific team helps maintain continuity during the review process. The roles of counsel, compliance officer, consultants, and other team members should also be clarified as part of project initiation.

The process and approach

Once a team has been appointed, its members must define and refine the process and approach. A critical initial component is to first review and gain an understanding of the current method for undertaking arrangement reviews. As part of this process, the team should be able to determine the individuals responsible for the daily management of physician arrangements. The purpose of the review must be clearly formulated, determining whether it is for internal audit purposes or for reporting requirements.

The contracts

One of the responsibilities of the review team is to locate all of the physician contracts and related supporting documents. For example, determining whether they are housed in a centralized repository, or decentralized among different departments, is critical to an efficient and effective review process.

The review sample

The team needs to determine the sample size, which should include a representative cross-section of contract types depending on the focus of the engagement, such as employment, medical director, personal services agreement, recruitment, facility lease, etc. With the sample selected, the contracts are then compiled for the review. This frequently includes generating a list of contracts from the contract management system by category pertaining to the scope of the review.

The supporting documentation

In order to complete the arrangements review, essential information is required, including:

- The contracts to review;
- Supporting written documentation, including but not limited to, items such as time sheets and needs assessments;
- Payment data from Accounts Payable and the Payroll department, including Form 1099 information;
- Related policies and procedures, for example:
  - Physician compensation philosophy

- ✧ Execution and controls for physician employment and personal services arrangements
- ✧ Management, payment, and auditing of physician compensation arrangements

Key items necessary for review are also further detailed later in the section, "A helpful checklist."

The project plan

A fundamental component to facilitating a successful physician arrangements review includes the development and execution of a formal project plan to help ensure that all parties involved do the following:

- ◆ Participate in regular team meetings and phone calls
- ◆ Establish a communications plan that helps team members efficiently share information
- ◆ Review pertinent findings throughout the process
- ◆ Use an arrangement review checklist that has been approved by legal counsel

The project plan will provide structure for the team members to follow a course of action to complete the review; document findings, questions, and the need for additional information; and report review results regularly to the team leader.

Process deliverables

When reporting the results of physician compensation arrangements reviews, it is important to provide details on the background, scope, approach, and a synopsis of the results. Detailing the discoveries sufficiently is critical in order to proceed with implementable action plans and prioritize each finding by evaluating the risk to an organization. Failure to do so in a meaningful way will stymie the ability of an organization to make the necessary process improvements. Any recommended corrective action should be based on the level of risk to an organization and the risk appetite of governance. Specifically, the review should identify any missing or deficient policies and procedures. Further, if a physician was compensated inappropriately, payment for any associated services must be analyzed to determine if repayments or refunds are required.

Any recommended corrective action should be based on the level of risk to an organization and the risk appetite of governance.

Apply best practices and strong internal controls

Organizations should be proactive and implement strong internal controls to guarantee that physician arrangements are executed properly when the contract is initiated, to potentially mitigate any compliance violations. They must also stay abreast of current regulations, maintain a process for receiving regulatory updates, develop a checklist to assure that proper processes are followed, and address all required elements appropriately. Further, they must justify the arrangements in order to pass outside agency scrutiny.

A basic control for any review of physician arrangements is that the agreement is signed by both parties. Although physicians who are bona fide employees do not require a written arrangement, having one can help document compliance with other required elements. Physicians who are not employed must have a signed written arrangement with the healthcare facility or organization before compensation is paid or services are performed, to avoid possible Stark violations.

Upon initiation, physician arrangements should be monitored regularly as part of the organizational compliance work plan. Written contracts must specify all services and items covered by the arrangements between the parties and must document circumstances that gave rise to an agreement. For example, a physician needs assessment or medical staff development plan can afford health facilities more latitude in offering incentives for physician recruitment and compensation based on the health needs of the community. Such assessment verifies the need for additional physician services or specialties and serves as part of an organization's efforts to comply with federal physician recruiting regulations.

Pursuant to the identified regulatory considerations, contracts must pay FMV compensation for the agreed-upon services. Regular reviews can help identify the need for correction of any excessive compensation arrangements. The total compensation for each physician should be market-based and reasonable in an economic sense. For example, arrangements in which a physician has more than one

contract with the same organization, or "stacked arrangements," can result in duplication of payment for the same services, triggering a "red flag" from both FMV and commercial reasonableness perspectives.

Regulatory oversight agencies require that payment arrangements are set in advance if physicians refer services to an organization with which they are under contract. For example, the compensation formula for independent contractors must always be set in advance and their compensation may not be adjusted retroactively. For personal services agreements, the aggregate compensation, not only the compensation formula, must be set in advance.

In addition, although there is a Stark exception for nonmonetary physician compensation, these benefits must be tracked and reported.[9] In general, the nonmonetary compensation exception may be used to protect items or services such as entertainment, meals, and other noncash equivalent benefits provided to a physician. Hospitals may provide nonmonetary compensation to physicians up to an aggregate amount of $407 for calendar year 2018. Additionally, the dollar limit for "incidental benefits" (e.g., meals, parking, use of internet) is less than $34 per occurrence. Hospitals should inventory such nonmonetary compensation and benefits to confirm they are meeting the law's requirements.

Finally, there should be an approved commercial reasonableness process in place. Documented best practices in support of a transaction make business sense in the absence of a referral stream.

Specifically, a proposed arrangement must demonstrate reasonable necessity to accomplish a rational business purpose. The particular nature of the duties and the corresponding amount of accountability under the proposed arrangement must be clearly defined and reasonable. In addition to other supporting factors, patient demands, the number of hospital patients, or the needs of the community must be sufficient to justify services.

Many healthcare organizations are not traditionally set up to manage the risks and address the uniqueness of physician compensation arrangements compliance. Employing best practices and robust internal controls can position the organization to mitigate significant compliance risks and to achieve assurance over operational effectiveness or regulatory compliance. Effectively designed, centrally managed, and periodically reviewed internal control functions are the single best method for maintaining regulatory compliance with physician compensation arrangements.

A helpful checklist

A physician compensation arrangement review checklist supports healthcare enterprises in taking the first steps toward initiating and managing physician compensation arrangements. The following critical elements can assist healthcare organizations when undertaking reviews:

- Establish physician classification—as an employee, contractor, or other
- Identify the duties the physician will provide, and whether any are duplicative
- Confirm that all parties have signed all agreements, and that they have legal counsel approval
- Ensure that the contract details the methodology for compensation
- Ensure FMV and commercial reasonableness assessments have been completed for any arrangement
- Determine whether the term of the contract is for at least one year, and whether it can be terminated without notice within one year
- Verify that the contract includes an annual performance evaluation and functional metrics that ensure that care, treatment, and services provided are administered safely and effectively
- Determine whether the contract requires the physician to document the delivered services and hours spent performing duties
- Review all supplemental compensation to determine if it is provided within the terms of the agreement
- Determine if physician payment aligns with the contract
- Prioritize physician compensation risks, including

In addition to other supporting factors, patient demands, the number of hospital patients, or the needs of the community must be sufficient to justify services.

stacked agreements and long-standing evergreen contracts
- Review real estate and equipment leasing agreements that involve physicians

Conclusion

As the number of employed and contracted physicians continues to increase, the regulatory and legal compliance of physician compensation arrangements will loom large, drawing further scrutiny from oversight agencies. Hospital and healthcare executives must expand their responsibility for oversight to assure that these arrangements provide fair, market-based compensation that complies with regulatory requirements. Contract development and implementation—as well as maintenance of supporting documentation, and regular, thorough reviews—are the fundamental components of a robust process to mitigate and prevent any potential compensation issues. CT

Endnotes

1. Anne Sharamitaro and Hal Goldsmith, "Recent False Claims Act Settlements Highlight Physician Compensation Scrutiny," Bryan Cave Leighton Paisner, September 23, 2015. https://bit.ly/2D8Msxc
2. 69 Fed. Reg. 16093, March 26, 2004. https://bit.ly/2Dmfyus
3. Department of Justice, Justice News press release, "National Health Care Fraud Takedown Results in Charges Against Over 412 Individuals Responsible for $1.3 Billion in Fraud Losses," July 13, 2017. https://bit.ly/2tMLth8
4. DOJ Justice News press release, "Former Employees of Southern California Ambulance Company and Dialysis Center Plead Guilty to Medicare Fraud Charges," November 27, 2017. https://bit.ly/2quDjrt
5. DOJ Justice News press release, "New Orleans Area Woman Sentenced to More Than Four Years in Prison for Role in Approximately $2 Million Home Health Kickback and Identity Theft Scheme" January 4, 2018, https://bit.ly/2QmqbA7
6. DOJ Justice News press release, "Miami-Area Man Sentenced to Five Years in Prison For Role in $63 Million Health Care Fraud Scheme," February 22, 2018. https://bit.ly/2qsXhTg.
7. DOJ Justice News press release, "Pharmacist and Pharmacy Employee Sentenced for Involvement in Over $30 Million Health Care Fraud," March 12, 2018. https://bit.ly/2OukHl7.
8. DOJ Office of the Deputy Attorney General, The Yates Memo, September 9, 2015. https://bit.ly/2nLMPa4
9. 42 C.F.R. § 411.357 (Exceptions to the referral prohibition related to compensation arrangements)

- Increasingly, healthcare organizations' business strategies include employing/contracting with physicians.
- Regulatory/legal considerations demand management's thorough oversight of physician arrangements.
- Physician arrangements are often complex and multifaceted.
- Regulatory/legal violations can invoke steep penalties and reputational damage.
- Technical reviews of physician arrangements/strong internal controls are critical.

HCCA 2019 REGIONAL

HEALTHCARE COMPLIANCE CONFERENCES

No matter where you live, *there we are*

With conferences in major cities in the United States, it is likely there is an affordable healthcare compliance conference ***within driving distance of your home or office***.

Join the Health Care Compliance Association in 2019 to learn and share compliance successes and challenges in your region. Learn from your peers, network, and earn CEUs.

Charlotte, NC | January 18
Atlanta, GA | January 25
Orlando, FL | February 1
Portland, OR | February 8
Dallas, TX | February 15
Anchorage, AK | February 21–22
St. Louis, MO | March 1
Washington, DC | March 8
New Orleans, LA | April 26
Columbus, OH | May 3
New York, NY | May 10
San Juan, PR | May 16–17
Philadelphia, PA | May 31
Seattle, WA | June 7
Los Angeles, CA | June 14
Ann Arbor, MI | June 21 NEW!
Boston, MA | September 6
Minneapolis, MN | September 13
Kansas City, MO | September 20
Indianapolis, IN | September 27
Pittsburgh, PA | October 4
Honolulu, HI | October 10–11
Denver, CO | October 18
Chicago, IL | October 25
Louisville, KY | November 1
Scottsdale, AZ | November 8
Nashville, TN | November 15
San Francisco, CA | December 6
Houston, TX | December 13
Richmond, VA | December 13 NEW!

hcca-info.org/regionals

Questions? amber.zerin@corporatecompliance.org

HCCA™ Health Care Compliance Association

HOW TO BUILD A POSITIVE RELATIONSHIP WITH YOUR CIA INDEPENDENT MONITOR

by J. Veronica Xu

J. Veronica Xu

Esq., CHC, CHPC, CCEP

(veronica.xu@saberhealth.com) is the Chief Compliance Office with Saber Healthcare Group, headquartered in Cleveland, OH.

When people hear an organization is currently under a corporate integrity agreement (CIA), they often give a sympathetic sigh and say "Aw, sorry to hear that." True, it is certainly not every organization's goal to have a CIA in place, but when you have one, I think the best approach is to face it, learn from it, and make the best of it. Once you fully understand it, you may even start to appreciate it and find great partners and resources from it.

In this article, I will mainly focus on what the independent monitor's (IM) responsibilities entail and what a long-term care (LTC) provider can do to build a positive relationship with its IM.

What is a CIA?

Many people are familiar with the term CIA, since it was introduced by the Office of Inspector General (OIG) within the Department of Health and Human Services (HHS) in the 1990s. CIAs are used as part of the civil settlement arrangement to resolve the allegations of fraud and abuse faced by healthcare providers. In exchange for the OIG's agreement not to seek an exclusion of the healthcare provider from participation in Medicare, Medicaid, and other federal healthcare programs,[1] the provider consents to the obligations as part of the civil settlement. The objectives of these CIAs are to improve the quality of the care that healthcare organizations provide to patients and residents, and to promote compliance with laws and regulations:

A comprehensive CIA typically lasts five years and includes requirements to:

- Hire a compliance officer/appoint a compliance committee;
- Develop written standards and policies;
- Implement a comprehensive employee training program;

- Retain an independent review organization to conduct annual reviews;
- Establish a confidential disclosure program;
- Restrict employment of ineligible persons;
- Report overpayments, reportable events, and ongoing investigations/legal proceedings; and
- Provide an implementation report and annual reports to OIG on the status of the entity's compliance activities.[2]

Whether your organization entered into a CIA with the OIG directly, or you inherited it through the acquisition of an entity that has one, you are required to comply with the obligations set forth therein, unless specified otherwise.

Other than the key elements of the compliance program, the specific requirements and obligations may vary slightly, because the CIAs are tailored to address certain issues identified in a particular setting, such as LTC providers, physicians groups, laboratories, pharmacies, etc. When a False Claims Act settlement resolves allegations of fraud that impact the quality of patient care, OIG may enter into a CIA with the provider. The CIA mandates that the provider retain an appropriately qualified monitoring team entity (the independent monitor) with clinical expertise to perform quality-related reviews.[3] The IM is selected by the OIG and will be responsible for assessing the effectiveness, reliability, and thoroughness of the provider's systems and procedures.

What exactly does the IM do?

The scope of review and responsibilities of the IM are set forth in the CIA. For LTC providers, the IM will typically review the following areas to determine whether the organization has effective and reliable measures in place to ensure the quality of care.

The organization's internal quality control systems:

- Whether there is a system in place and whether it is implemented in a timely and effective manner;
- Whether there is an internal communication system and whether it is effective; and
- Whether there are effective, thorough, and competency-based training programs.

The organization's quality of care:

- Whether the organization is able to identify issues;
- Whether it can determine the scope of the issues, including whether the issue is isolated or widespread;
- Whether the organization has the ability to analyze outcome measures, such as the CMS Quality Indicators and other data;
- Whether there is a quality-of-care dashboard that establishes overall quality improvement goals, quality indicators, and performance metrics based on the risk areas;
- Whether the organization is capable of conducting a root-cause analysis;
- Whether it can develop an action plan in response to the issues; and
- Whether it has the ability to monitor and evaluate its assessment, action plan, and execution of the plan.

Staffing:

- Whether there are programs and measures in place to enhance employee recruitment and retention;
- Whether the organization's staffing committee is effective in identifying issues and addressing concerns; and
- Whether the organization is in compliance with staffing requirements.

The IM is selected by the OIG and will be responsible for assessing the effectiveness, reliability, and thoroughness of the provider's systems and procedures.

Rehabilitation therapy system:

- Whether the therapy service delivered is in line with the physician's order and with an individualized plan of care;
- Whether the treatment is consistent with the nature and severity of the resident's individual illness or injury;
- Whether the care provided is in compliance with accepted standards of medical practice;
- Whether the therapy is reasonable and necessary to improve a resident's current condition, to maintain the resident's current condition, or to prevent or slow further deterioration of the resident's condition;
- Whether therapy is limited to services that require the

skills of physical, speech, and/or occupational therapists and whether resident safety is maintained and the medically desired result is achieved;
- Whether the organization is tracking therapy minutes in accordance with the Medicare program requirements; and
- Whether appropriate documentation of medical records is properly maintained in compliance with Medicare guidance.

In fact, all of these elements are not completely new to LTC providers. Healthcare providers have long been under much of the scrutiny from governmental agencies. CIAs simply formalize those practices that many LTC providers have been following and reduce them to writing. Those structured processes provide valuable guidance to providers and help them stay on the right track.

In order to effectively carry out its responsibilities and accurately reflect the organization's compliance performance, the IM usually does the following, among other things:
- Reviews various reports and information that the organization submits, including monthly reports, clinical records, meeting minutes, training documentation, program information, etc.;
- Visits the facilities periodically to observe care delivery; and
- Attends meetings of all levels within the organization, including care planning meetings at the facility level, staffing committee meetings, compliance committee meetings, board of director meetings, etc.

Under the CIA, the IM is generally entitled to immediate access, at any time, and without prior notice, to your organization's facility site(s) and your data, reports, surveys, complaints, records, and anything that the IM deems relevant. In addition, the IM can interview residents and employees without the presence of any supervisory staff or counsel. Furthermore, on a quarterly basis, the IM will reassess the systems' effectiveness, reliability, and thoroughness.

Building a strong relationship and cultivating positive interactions

Naturally, the IM will be working with the organization for the same period of time, unless otherwise specified or required by the OIG. Although the IM is not an agent of the OIG, they communicate with the OIG periodically and report information about the organization's compliance performance to the OIG. Whether you like it or not, while the CIA is in effect, the IM is there with you.

Is it intense to work with an IM? It can be. Does it have to be miserable? Absolutely not. People often say, life is as good as you make it. I would like to think that the IM is the organization's partner. In fact, they are a great resource because, as a neutral party from the outside, the IM can sometimes see things with a set of fresh eyes and from a different perspective that the organization could have easily missed. True, IMs are appointed by the OIG to monitor the organization, but it should be recognized that they are not only there to assess and audit, but also to provide guidance and help your organization be better. So, why not make it count?

Best practices and tips

Building a strong relationship with the IM and having positive interactions with them can help make things go smoothly. Below are some tips and best practices that may benefit an organization that is under a CIA.

Be open-minded

Generally, organizations that are under a CIA have systemic failures, whether relating to clinical care, therapy treatment, billing, or staffing issues. Thus, it is not surprising that the IM will find many issues, especially at the beginning of the CIA term. When they hand you over a long list of things that you did wrong, now what? People don't usually like to be told what they did wrong. It is part of human nature to defend and resist. It takes courage to face and accept criticisms; and it takes wisdom to appreciate, reflect, and act upon them. Being open-minded and receptive does not mean blindly accepting all comments or opinions. The point is, with the right mind-set, the IM's input and findings will help the organization to re-evaluate its practices and rethink its approach.

Be positive

Having a positive attitude is crucial. I've heard people say, attitude determines personality and personality determines destiny. In my opinion, the same holds true for an organization. For example, when the IM points out an issue with the organization's infection control program, they are helping the organization identify an issue that it overlooked, thereby helping it improve its infection control program and prevent potential outbreaks among patients and residents. For another example, when the IM finds that your organization did not effectively publicize your hotline information, they are reminding you of the importance of reaching out to your employees and

sharing reporting mechanisms with them. When an employee reports a concern to an internal authority, we should thank the employee, because he/she is giving the organization an opportunity to address the issue and correct the error internally, if applicable.

Be transparent

To error is human. No one is perfect and IMs understand that. In the healthcare setting, we work with people. The fact is, people make mistakes and things do happen. When there is an error or an incident—especially a grave one involving resident care and safety—rather than trying to hide it from the IM, it is important that the organization be transparent. It is always good to voluntarily share critical information with the IM, not only because they have access to the organization's data and would know it anyway, but also because it is one of the requirements under the CIA that the organization notify the IM of any reportable events. It should be noted that it is not the IM's goal to punish the organization; rather, they are there to assess the organization's ability to handle situations properly when bad things happen. Therefore, a better way to handle it is: In addition to the information about the incident, the organization can also share what it had done to remediate the issue (e.g., following the identification of the issue, the organization conducted a root-cause analysis and properly addressed it in a timely manner).

Be collaborative

Although it is the IM's duty to examine the effectiveness of the compliance process and to measure progress, their goal is no difference than ours—that is, to ensure patients and residents receive the quality care that they deserve. In order for it to work, it should not be an adversarial relationship. It is always easier said than done, but how will you be collaborative? First of all, be a good communicator. Communication is key to the success of any relationship, whether it's between spouses, partners, colleagues, etc. For example, the organization should keep open lines of communication through periodic conference calls, in-person meetings, and written communications. So far in my career, I have been fortunate enough to have met and worked with many wonderful, individual IMs. They are very reasonable, knowledgeable, and understanding. They are willing to share their insights with you. When you demonstrate that your organization truly respects the IM and is willing to work with them to improve the quality of care, the IM appreciates it, and you have established a great partnership.

Be proactive

Having an IM is an external resource as well as a CIA requirement, but it cannot replace the organization's internal review and self-audit. In addition to responding to the IM's oversight and auditing, the organization should stay proactive and continuously examine its own systems to identify any issues and to evaluate the system's effectiveness. Based on the issues and deficiencies identified, the organization should periodically review/modify its procedures and processes, and update the IM on its progress and findings.

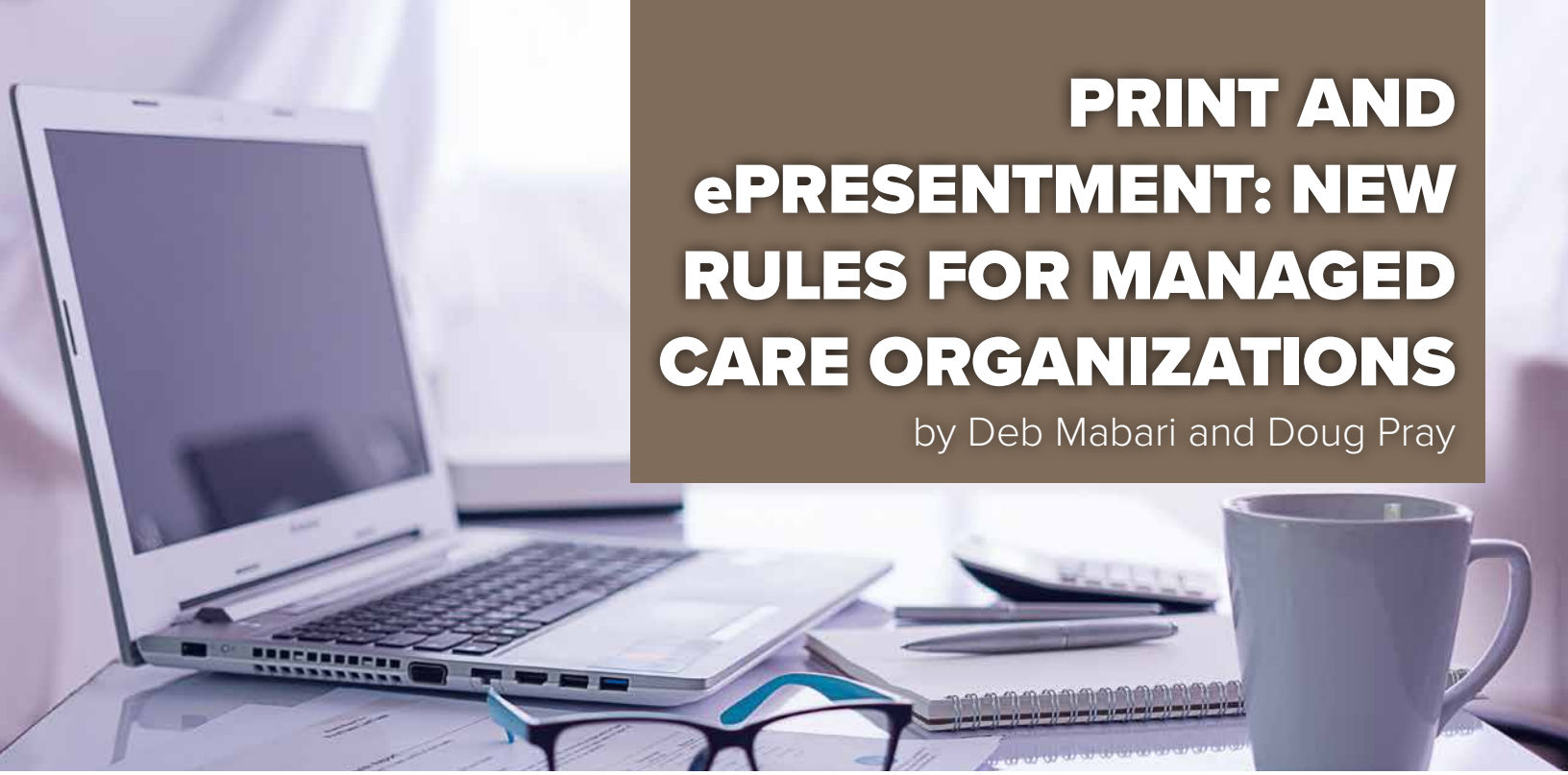
Conclusion

Although it is not fun to have a CIA, it truly is a great learning experience for the organization in terms of formalizing its processes and procedures, enhancing its quality control and compliance programs, and improving clinical care and outcomes. Understanding the IM's responsibilities will certainly help the organization meet the CIA requirements. By following the aforementioned tips and best practices, it will help the organization go a long way.

Endnotes

1. The Office of Inspector General, Corporate Integrity Agreements. https://bit.ly/2OUfAKZ
2. Idem
3. The Office of Inspector General, Quality of Care Corporate Integrity Agreements. https://bit.ly/2FMlRJF

- Knowing what the independent monitor's (IM) responsibilities entail will help you better understand and meet CIA requirements.
- Having an open mind and a positive attitude is crucial in building a strong relationship with the IM.
- Transparency is essential when working with the IM.
- It should be a collaborative relationship, not adversarial.
- The organization should stay proactive and continuously examine its own system to identify issues and assess its effectiveness.



PRINT AND ePRESENTMENT: NEW RULES FOR MANAGED CARE ORGANIZATIONS

by Deb Mabari and Doug Pray

Deb Mabari

Doug Pray

Deb Mabari *(dmabari@codyconsulting.com) is Chief Executive Officer and* ***Doug Pray*** *(dpray@Codyconsulting.com) is Director, CodyPrint®, CODY in Tampa, FL.*

In October 2017, Centers for Medicare & Medicaid Services (CMS) Administrator Seema Verma announced an initiative called Patients over Paperwork.[1] The initiative focused on streamlining regulation to reduce unnecessary burdens on health plans and providers, as well as increasing efficiencies and improving the member experience. In April 2018, the CMS Final Rule for Contract Year (CY) 2019[2] incorporated policy changes driven by the Patients over Paperwork initiative that allows Medicare Advantage and Part D plan sponsors to provide specific types of plan information, such as the Evidence of Coverage (EOC) electronically instead of in hard copy.

Under the final rule, the Annual Notice of Change (ANOC) and the EOC documents are now two independent documents with different delivery requirements and flexibilities. This may seem like a simple change, but it requires serious thought and planning by health plans. It is imperative that health plans pay attention to these changes.

Benefits for health plans

Beginning with CY 2019, ANOCs and EOCs no longer need to be combined in the mailing due to members by September 30 each year. Health plans now have until October 15 to provide EOCs electronically. The ANOC must continue to be delivered by September 30 each year, which is 15 days prior to the Annual Election Period (AEP), and must be received by enrollees ahead of the EOC, allowing enrollees to "focus on materials that drive decision-making during AEP" as CMS suggested in the final rule.

CMS estimates this new rule has the potential to save health plans $54.7 million a year from 2019 through 2023.[3] These savings will come from eliminating or significantly reducing expenses related to printing, fulfillment, and mailing costs (e.g., paper, prepress and printing, bindery, lettershop, USPS postage, logistics carriers) for the EOCs.

Beyond the monetary savings, health plans now have more time to produce the EOCs. In addition to having two more weeks until these documents are due to members, health plans that provide EOCs electronically also free up part of the timeline previously

dedicated to prepress, printing, and mailing of the EOC books.

Health plans must use the extra time wisely

CMS has explicitly stated that the extra time for EOC creation "will also provide an additional two weeks for MA [Medicare Advantage] organizations and Part D plan sponsors to prepare, review, and ensure the accuracy of the EOC, provider directory, pharmacy directory, and formulary documents."[4] Health plans need to use the time wisely and get these documents right the first time, or be prepared for fines and sanctions from CMS.

Some health plans may quickly realize that the extra time to create these documents is a mixed blessing. They must allow additional time for document review from all participating departments, including Marketing, Product, and Compliance. Review of required documents must include all stakeholders and departments in an in-depth review of content pertaining to members' plan benefit information, co-pays by drug tier, and phone numbers and TTY, just to name a few.

Health plans need to take an enterprise-wide approach in their review process. Other departments, including, but not limited to, Operations, Pharmacy, Provider Network, Call Center, Health Services, Long-Term Care (LTC), and Claims, must be brought into the review process to ensure 100% accurate documents. This exercise should be like the one that happens annually during a health plan's annual budgeting process.

Create a single "Source of Truth"

Every health plan will have its own process for reviewing and comparing materials annually to ensure accuracy. One of the best ways to start the review process is to analyze and compare current CMS Model Documents[5] to the prior year's documents. A full understanding of the changes in all plan types from year over year is essential. This review can be done by mapping the plan benefit package (PBP) report to variable data fields and addressing the variability in the templated documents.

Although there are several products on the market that can help health plans do this mapping, it is essential that you work with a firm that has a broad-spectrum, hands-on understanding of the nuances of these reports across many plan calendar years. This is not a process that can just be managed by writing a query. The data produced at the end of this process becomes an invaluable input into creating the EOCs (and various other documents) and should be considered a health plan's annual "Source of Truth." This output will contain all the updated plan benefit information for the new year. If this mapping from the PBP report is not done correctly, all plan benefit and ancillary information could (will) be wrong, creating erroneous materials.

When changes are required during the materials creation process, changes to the single, centralized Source of Truth can be made and disseminated throughout the organization immediately. This is a critical step in the creation process. It keeps all departments and team members updated to any changes, which is essential to the goal of 100% accuracy. Effective communication is key.

Allow ample time for all departments to review

During the review process, allowing ample time for your subject-matter experts (SMEs) to review the data in the Source of Truth, templates, and final version documents is imperative. Many changes can occur during this process, and maintaining version control is *key*. It may sound simple, but it's not.

Your Pharmacy department may want to change language it does not like in a single version of an EOC, but it may not be a viable option to do so. This version was likely created using the most recent Model Documents provided by CMS, and CMS-compliant documents mean model language cannot be changed. The decision to move from model to non-model language should be made only by the Compliance department, because it could significantly impact the submission and review/approval process by CMS's Regional Office (RO).

Opt-in or opt-out

As noted, once the documents are created, approved, and submitted as final, CMS permits the electronic delivery of many materials (for this article, we will refer to any electronic delivery as ePresentment). CMS defines two distinct processes for ePresentment in Section 100.2.1 and 100.2.2 of the Medicare Communications and Marketing Guidelines (MCMG).[6]

The first is through a Notification of Availability or notice that tells the enrollee how to access designated materials on plan website(s) and gives the date that the materials will be available (or states that the materials are currently available). At minimum, health plans must also provide a phone number by which the member can opt-out of electronic delivery and request a hard copy version of the document. Updates to the CY 2019 MCMG on September 5, 2018, also state that if the member

requests a hard copy/printed version of a document, that "Plans/Part D sponsors may inquire to the member whether the request for a hard copy is a one-time request or is a request to receive the document in hard copy permanently."

The second option for ePresentment of materials requires prior consent from the member, or opt-in. With prior consent, health plans can provide any required materials through a member portal, email, or CD/DVD.

The use of member portals, email, and other delivery methods…requires the health plan to obtain consent from the enrollee to receive the materials…

The first process for ePresentment detailed above requires only prescribed notification of access and availability. The use of member portals, email, and other delivery methods for presenting materials to members requires the health plan to obtain consent from the enrollee to receive the materials, with specificity as to the media type or mechanism for ePresentment. In addition, a member must also have continued access to a mechanism for opting out or withdrawing the opt-in consent and reverting to hard copy receipt of materials upon request.

When a member opts in to ePresentment via email or a member portal, health plans must ensure that the member's contact information is current and can track electronic delivery of the materials with a time/date stamp recorded for each access point. If the transmission fails, due to an expired email address, connectivity issues, or other reasons, health plans must have a mechanism in place for automatic opt-out conversion of the member status, and a hard copy must be printed and mailed.

ICT Refresh and Revised 508 Standards

In 1998, the Workforce Investment Act[7] introduced amendments to the Rehabilitation Act of 1973. Included in these amendments was a new Section 508,[8] which required all federal agencies to ensure that their electronic and information technology was accessible to people with disabilities. Critical to our discussion of present-day standards was the requirement that "individuals with disabilities, who are members of the public seeking information or services from a Federal department or agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities."[9]

In December 2000, the U.S. Access Board introduced a set of accessibility standards, definitions, and guidelines that federal agencies would reference to comply functionally and technically with Section 508.[10] This set of standards and guidelines was the reference point for federally contracted healthcare and health insurance providers until January 18, 2017, when the Information and Communication Technology (ICT) Refresh[11] was published as part of the final rule that jointly updated requirements for information and communication technology.

The ICT Refresh, formally known as the ICT Standards and Guidelines, revised and updated the original Section 508 standards and codified them through the incorporation of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG),[12] a globally recognized standard for web content and ICT. For a comparison table of the "old" 508 standards to the WCAG 2.0 A and AA standards, visit *https://bit.ly/1ToCnj1*.

With the incorporation of WCAG 2.0 AA standards set into Section 508 via the ICT Refresh, website, document, and media developers now have a specific set of success criteria for making web content accessible to a wide range of people with disabilities, including blindness, visual impairment, color blindness, deafness and hearing loss, and learning and cognitive limitation.[13] Critically, the success criteria that are part of the WCAG 2.0 standard set are testable. Auditing of websites and web-based materials can now be done objectively using software specifically designed for that purpose.

This background information is important from a compliance perspective because since January 18, 2018, every health plan website and all digital content must meet the testable WCAG 2.0 AA standards. CMS is now allowing more member-facing documents to be electronically presented, which presents website and content managers with a new and significant challenge—how to make sure that electronically presented PDF documents meet or exceed the WCAG 2.0 AA success criteria. Keep in mind that although the ICT Refresh currently incorporates WCAG 2.0 AA into the final rule, W3C has now updated the WCAG 2.0 standard with WCAG 2.1, which contains an additional 17 new

criteria, so this requirement is likely to get more stringent over time.

Creating and testing accessibility for ANOC, EOC, Formulary, Directory, Summary of Benefits, and other PDF documents available on health plan or provider sites is paramount before publishing these documents. Organizations that use downstream vendors for remediation of PDF documents should always ask for definitive and detailed reports showing that a PDF passes all WCAG 2.0 AA checkpoints before publishing. Federal auditors now have several specific software tools that can be used to check website and content accessibility.[14] Securing the services of a reputable authority to remediate Plan PDF documents should be a top priority.

Questions for health plans to consider

Armed with the information and perspectives shared above, the following questions may be helpful for determining whether your health plan is prepared to comply with the new print and ePresentment rules:

- Does the EOC Request Notice that is sent with the ANOC mailing contain a specific, variable URL (web link) for each electronically presented document within a PBP, or does the notice simply direct members to the Plan Documents section of the website, and have the member select their specific EOC document based on the health plan's name? How does a health plan ensure that a member accesses and references the correct PDF document?
- Do health plans need to create or update their member portal infrastructure? Plans should make it as easy as possible for members to find their specific documents.
- If a member opts out of receiving their electronic document(s), how do health plans document that members have opted out?
- How do health plans tie the opt-out notice to each member's record so that a call center representative can easily find the document when a member calls, thereby enabling a more positive customer service experience?
- How will health plans ensure that their website and the electronic documents, including EOCs, are compliant with Section 508 and the WCAG 2.0AA standard?
- How are printed copies of EOCs and other ePresentment documents made available to members who request them?
- Have Customer Service and Marketing managers developed efficient and scalable processes to compile and verify member request data?
- Do health plans print a limited number of copies to pull from the shelves, or will they use on-demand printing and fulfillment to meet the three-day rule for fulfillment of requested hard copy materials?

Conclusion

Health plan fulfillment is a changing landscape in the face of new electronic presentment and accessibility rules. Health plans must be vigilant and diligent about keeping abreast of these changing rules and guidance as we transition more and more to digital and online fulfillment practices. CT

Endnotes

1. Centers for Medicare & Medicaid Services (CMS), Patients over Paperwork. https://go.cms.gov/2P4RjWJ.
2. Federal Register/Vol. 83, No. 73 CMS, Medicare Program, Contract Year 2019 Policy and Technical Changes to the Medicare Advantage, Medicare Cost Plan, Medicare Fee-for-Service, the Medicare Prescription Drug Benefit Programs, and the PACE Program, 2018. https://bit.ly/2DBpwr0
3. Idem at 16441.
4. Idem at 16622, http://bit.ly/2QYoKaU
5. CMS, Marketing Models, Standard Documents, and Educational Material. https://go.cms.gov/2Oq50zY.
6. CMS, *Medicare Communications and Marketing Guidelines* (MCMG), September 5, 2018. https://go.cms.gov/2P7PU1w.
7. United States Department of Labor Employment and Training Administration, Workforce Investment Act of 1998. https://www.doleta.gov/regs/statutes/wialaw.pdf.
8. U.S. General Services Administration (GSA), IT Accessibility Laws and Policies, Section 508 of the Rehabilitation Act of 1973. http://bit.ly/2CnaGUp.
9. United States Access Board, The Rehabilitation Act Amendments (Section 508), § 794 (d). http://bit.ly/2J0n0v1.
10. United States Access Board, Section 508 Standards for Electronic and Information Technology. http://bit.ly/2Eo9oLi.
11. Federal Register, Vol 82, No. 11, Information and Communication Technology (ICT) Standards and Guidelines, January 18, 2017. http://bit.ly/2OqCkXH.
12. Web Content Accessibility Guidelines (WCAG) 2.0. http://bit.ly/2QRLeKD.
13. United States Access Board, About the Update of the Section 508 Standards and Section 255 Guidelines for Information and Communication Technology. http://bit.ly/2NN5VoW.
14. GSA Section 508.gov, Accessibility Testing for Electronic Documents. https://www.section508.gov/test/documents.

- Take the time. Prepare and have a plan.
- Create a centralized, plan benefit package-based "Source of Truth."
- Review, review, review—use your subject-matter experts wisely.
- Adhere to all CMS mandates and guidelines.
- Be mindful, and make sure that you have the proper policies and procedures in place to ensure accuracy.

HCCA

HIPAA/HITECH/Privacy/Security

Home health and Hospice

Hospitals, Health Clinic, and Healthcare Systems

Investigations

Letter from the CEO by Roy Snell

Letter from the Incoming CEO by Gerry Zack

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)®

- Bethany Moss
- Swigah Mwakipake
- Teresa Nash-Hampton
- Tyre Nelson
- Jerry Aloysius Newman
- MaryAnn Northrup
- Elizabeth Owen
- Catherine Patsos
- Daniel Peake
- Maria Penate
- Valree Peralta
- Heather B. Perrin
- Michelle I Pinter
- Robert F. Porr
- Edwin Punsalan
- Sally Rainer
- Melony A. Rarick
- Melissa Reinders
- Jessica Rod
- Ashley L. Rodriguez
- Vanessa Rops
- Julie M. Roumillat
- Carrie Ruby-Geiger
- David Samar
- Ruth Schimmel
- Nina Shah
- Carol Slovacek
- Kacie Smith
- Darren L. Speed
- Rachel Stevens
- Allison Swartz
- Elizabeth A. Taylor
- Kathy Thomas
- Tammy G. Towers
- Talisha Williams
- Vicki Wireman
- Debbie Yoder
- Kathleen Zitzman
- Patricia Zuercher

Certified in Healthcare Privacy Compliance (CHPC®)

- Christina Batress
- Jason Beard
- Robyn G. Blache
- Marilyn H. Boston
- Andrea L. Britt
- Susy Cabrera
- Sean C. Campbell
- Torrey J. Clark
- Donna Cunningham
- Anne S. Daly
- Jeanine Dressler
- Brandon Dycus
- Daniel Elmlinger
- Thom Goodwin
- Daniel J. Goulart
- Ellen J. Gribbin
- Tomoyuki Hata
- Tammy L. Hawkins
- Anna Holtzhauser
- Mari Howard
- Alyssa Hunt
- Dana F. Jones
- Pamela F. Kendrick
- Melody L. King
- Jonathan Klock
- Heather M. Landreville
- Clinton Mayes
- deAnne McCoy
- Stacie McCutcheon
- Teresa M. McMeans
- Vicki L. Moody
- Melissa Price
- Peter Rill
- Sherri Roberts
- Andrea Rotella-Lamb
- Joy Royes Page
- Audrey St. John
- Scott Sumrall
- Megan Tharp
- Brenda Tirsun
- Mila C. Todd
- Josh C. Waltrip
- Jacqueline Yarbrough

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

***Shannon Sumner,* CPA, CHC**
Consulting Principal
PYA
Brentwood, TN

Why did you decide to get certified?

Although I've worked in the healthcare internal audit and compliance fields for over 20 years, I felt that specific certification in healthcare compliance, combined with the fact that the certification is through a highly respected organization, would solidify my credibility in the profession.

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

Although I am an owner in one of the largest healthcare consulting firms in the U.S., having the CHC certification communicates to our clients that I have the expertise they are expecting us to provide. Several of our compliance consultants are Certified in Healthcare Compliance, and we encourage and support others to obtain the certification.

Would you recommend that your peers get certified?

Definitely. Although it had been a while since I had sat for any type of exam, preparing for the CHC exam reinforced key concepts I knew, but also identified areas for additional research. Attending the various HCCA events and reading HCCA's weekly *Report on Medicare Compliance* newsletter makes it easy to stay certified!

CHC™
CERTIFIED IN HEALTHCARE COMPLIANCE

Managed Care
Compliance Conference

January 27–30, 2019 | Lake Buena Vista, FL

Attend the annual education & networking event for those who manage compliance for health plan providers.

REGISTER TODAY!

Delve into compliance hot topics and issues, including risk adjustment, CMS compliance, ethical leadership, data security, audits, and the challenges of the job. You'll learn the latest practices, share strategies, and connect with peers and mentors who work in the industry. The optional Certified in Healthcare Compliance (CHC)® exam is offered on the last day. Separate application and fee required.

hcca-info.org/managedcare

Questions? taci.gregory@corporatecompliance.org

HCCA™
Health Care Compliance Association

Takeaways

January 2019

COMPLIANCE TODAY
A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

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

Workplace violence: What compliance professionals should know about the unthinkable

Amy S. Garner (page 18)

- Healthcare workers are four times more likely to be involved in a workplace violence incident than workers in other industries.
- Compliance and privacy officers may not realize the importance of being prepared for incidents of workplace violence.
- Compliance and privacy officers should prepare for both internal and external investigations immediately following incidents of violence.
- Hospitals in particular are required to comply with various regulations and standards that may be implicated when a tragic incident occurs.
- Hospitals should assign primary contacts for each regulatory agency that requires information related to an incident of workplace violence.

Controlling mobile devices in an academic medical center: Unique challenges

Marti Arvin (page 22) CEU

- Information security and privacy challenges are present in all healthcare organizations.
- Academic medical centers (AMCs) may have additional challenges not present in other healthcare organizations.
- Understanding what academic freedom is, versus what it is not, is key.
- There are regulatory enforcement agencies beyond OCR to consider.
- Coordinating efforts between multiple parties will increase the success of the AMC's information privacy and security program.

Compliance tips for implementing an electronic medical record system

Lisa I. Wojeck (page 28)

- Electronic medical record (EMR) system project leads may not be aware of compliance issues.
- Improperly built EMR systems may cause the covered entity to incur fines and/or penalties.
- Electronic communications outside the EMR system between physicians and patients raise more than privacy issues.
- Although EMR systems may be very good for electronic medical record purposes, they may be limited for other purposes.
- Compliance professionals are valuable resources to covered entities as they make business decisions about their EMR system.

Tried and true survey readiness

Jennifer Ann Yang (page 34)

- Survey readiness should be continuous and operate year-round.
- Survey readiness is a facility-wide effort and requires a team-oriented approach with leadership support.
- Survey readiness requires extraordinary organizational skills and robust tracking tools.
- Facilities should develop a functional command center for the week of the survey to coordinate and track all survey activities.
- Successful survey readiness takes practice, training, and overall cultural change.

Got privilege? Best practices to protect privileges during an internal investigation

James Holloway (page 42)

- Be sure to have in-house or outside counsel lined up at the start of an internal investigation.
- Legal counsel should retain the experts who will be assisting with an investigation.
- Label materials as "privileged" to alert recipients to safeguard the materials, but do not expect that label to protect non-privileged information.
- Be careful when forwarding or sharing privileged information to avoid waiving privileges.
- Disclosing privileged information outside the company should only be considered after consulting with legal counsel.

Payment collection controls

Darryl Rhames (page 46)

- Ensure accuracy and reliability of captured financial information.
- Implement physical and system controls to safeguard assets.
- Develop a company-wide training program.
- Create audit tools, such as questionnaires, to monitor payment activity.
- Use walk-throughs to help detect and prevent fraud.

New CMS rule revisions affecting your inpatient rehabilitation facility

Danielle C. Gordet (page 52) CEU

- The post-admission physician evaluation may count as one of the three face-to-face physician visits in the first week of a patient's inpatient rehabilitation facility (IRF) admission.
- The rehabilitation physician may now lead the interdisciplinary team meetings remotely via video or telephone conferencing.
- CMS removed the IRF admission order documentation requirement; however, to be considered an inpatient, a patient is still required to be formally admitted as an inpatient under an order for inpatient admission.
- CMS is considering future policy changes that would give rehabilitation physicians the flexibility to conduct some IRF patient visits remotely.
- In the future, CMS may allow non-physician practitioners to play a greater role in IRF care, thereby removing some of the requirements placed on rehabilitation physicians.

Physician compensation arrangements: Robust reviews are a must

Tynan O. Kugler and Susan Thomas (page 56) CEU

- Increasingly, healthcare organizations' business strategies include employing/contracting with physicians.
- Regulatory/legal considerations demand management's thorough oversight of physician arrangements.
- Physician arrangements are often complex and multifaceted.
- Regulatory/legal violations can invoke steep penalties and reputational damage.
- Technical reviews of physician arrangements/strong internal controls are critical.

How to build a positive relationship with your CIA independent monitor

J. Veronica Xu (page 64)

- Knowing what the independent monitor's (IM) responsibilities entail will help you better understand and meet CIA requirements.
- Having an open mind and a positive attitude is crucial in building a strong relationship with the IM.
- Transparency is essential when working with the IM.
- It should be a collaborative relationship, not adversarial.
- The organization should stay proactive and continuously examine its own system to identify issues and assess its effectiveness.

Print and ePresentment: New rules for managed care organizations

Deb Mabari and Doug Pray (page 68)

- Take the time. Prepare and have a plan.
- Create a centralized, plan benefit package-based "Source of Truth."
- Review, review, review—use your subject-matter experts wisely.
- Adhere to all CMS mandates and guidelines.
- Be mindful, and make sure that you have the proper policies and procedures in place to ensure accuracy.

HCCA Upcoming Events

JANUARY

January 18
Atlanta Regional Conference
Charlotte, NC

January 21-24
Basic Compliance Academy
Lake Buena Vista, FL
CHC Exam

January 21-24
Healthcare Privacy Academy
Lake Buena Vista, FL
CHPC Exam

January 25
Atlanta Regional Conference
Atlanta, GA

January 27-30
Managed Care Compliance Conference
Lake Buena Vista, FL
CHC Exam

January 9
Web Conference
Negotiation Tips + Tricks (budget + contract)

January 17
Web Conference
Disaster Recovery and Business Continuity

January 22
Web Conference
Why is the Code of Ethics important

FEBRUARY

February 1
Orlando Regional Conference
Lake Buena Vista, FL

February 4-7
Basic Compliance Academy
Scottsdale, AZ
CHC Exam

February 8
Portland Regional Conference
Portland, OR
CHC Exam

February 18-19
Board & Audit Committee Compliance Conference
Scottsdale, AZ

2019

Managed Care Compliance Conference
January 27–30 • Orlando, FL

Board & Audit Committee Compliance Conference
February 18–19 • Scottsdale, AZ

23rd Annual Compliance Institute
April 7–10 • Boston, MA

Research Compliance Conference
June 9–12 • Orlando, FL

Clinical Practice Compliance Conference
October 27–29 • Nashville, TN

Basic Compliance & Ethics Academies
January 21–24 • Orlando, FL
February 4–7 • Scottsdale, AZ
March 18–21 • Chicago, IL
April 15–18 • San Diego, CA
May 13–16 • Minneapolis, MN
June 3–6 • Washington, DC
June 17–20 • New Orleans, LA
July 22–25 • Denver, CO
August 5–8 • New York, NY

Healthcare Privacy Basic Compliance Academies
January 21–24 • Orlando, FL
March 11–14 • Chicago, IL

Research Basic Compliance Academies
March 11–14 • Chicago, IL

Regional Compliance & Ethics Conferences
January 18 • Charlotte, NC
January 25 • Atlanta, GA
February 1 • Orlando, FL
February 8 • Portland, OR
February 15 • Dallas, TX
February 21–22 • Anchorage, AK
March 1 • St. Louis, MO
March 8 • Washington, DC
April 26 • New Orleans, LA
May 3 • Columbus, OH

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

APRIL 7–10, 2019 • HYNES CONVENTION CENTER

Don't miss these topics

711 Experiencing the Unimaginable: A Compliance Case Study of the Mass Shooting in Las Vegas

Susan M. Pitz, General Counsel,
University Medical Center of Southern Nevada

Keith Slade, Privacy Officer,
University Medical Center of Southern Nevada

Rani Gill, Compliance Officer,
University Medical Center of Southern Nevada

207 Navigating the Changing Regulatory and Enforcement Landscape Relating to Opioids

Anna Grizzle, Partner,
Bass, Berry & Sims PLC

Tizgel High, Vice President,
Associate General Counsel, Legal,
LifePoint Hospitals

Jerry Williamson, Healthcare Consultant

P11 Launching Ladies into Senior Leadership

Kristy Grant-Hart, Owner,
Spark Compliance Consulting

Jenny O'Brien, Chief Compliance Officer,
UnitedHealthcare

Kirsten Liston, Principal, Rethink Compliance

114 Blockchains Technology: Move Fast and Break Things Reconsidered

Scott Streibich, Director, Research Compliance Operations, Johns Hopkins University

110 Conducting a Behavioral Health Risk Assessment

Tim Timmons, Privacy and Security Officer,
Greater Oregon Behavioral Health

Todd Jacobson, Corporate Compliance Officer,
Greater Oregon Behavioral Health, Inc.

Pricing promotion extended

Register by January 22

Register at compliance-institute.org

Questions? jennifer.parrucci@corporatecompliance.org

HCCA™
Health Care Compliance Association